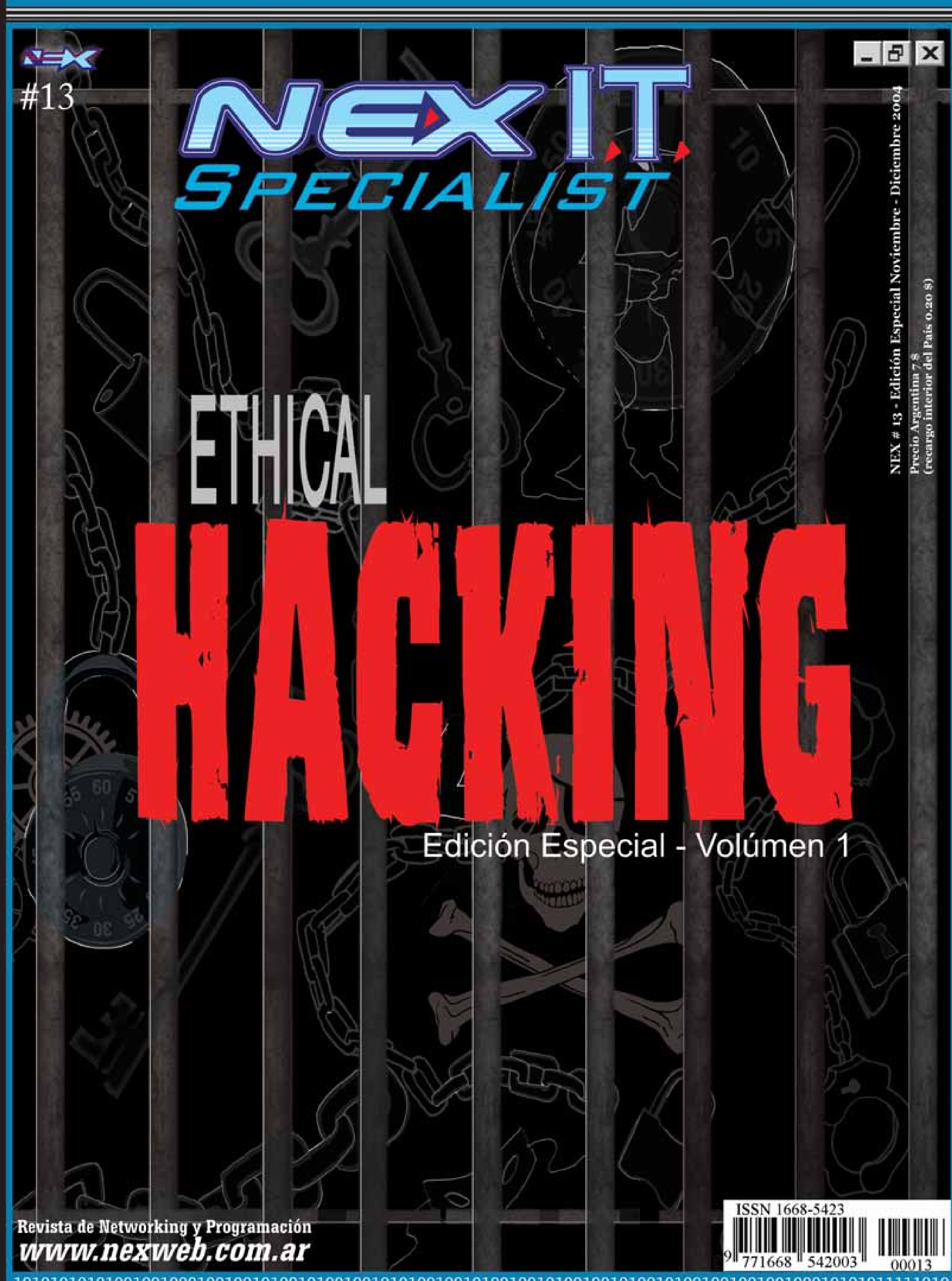


NEX
#13
NEX I.T. SPECIALIST
ETHICAL
HACKING
Edición Especial - Volúmen 1
NEX # 13 - Edición Especial Noviembre - Diciembre 2004
Precio Argentina 7 $
(recargo interior del País 0.20 $)
ISSN 1668-5423
9 771668 542003 00013
Revista de Networking y Programación
www.nexweb.com.ar
10101010101001001000100100101001010010010101001001010010010100100101001010010010010010001010101111110




Editorial

Hace muchos años la enseñanza del inglés se realizaba de un modo muy aburrido. Se hacía mucho hincapié en la gramática y las estructuras.

Eso se modificó, hubo un cambio drástico, cambiando a una enseñanza basada en ejemplos cotidianos, divertidos.

Con los libros de seguridad informática de hoy sucede algo parecido. Son en general libros áridos. Pueden ser muy buenos, pero su lectura resulta, en general, "aburrida".

Existe un segundo ingrediente y es que en general están tan llenos de información que uno pierde el panorama general, al menos que se disponga del tiempo para recorrer todo el libro.

En "Ethical Hacking" Volumen 1 y 2, que tendrá en sus manos junto a las próximas 2 ediciones especiales de "NEX IT Specialist", Ud. encontrará una propuesta diferente:

1. el contenido se ha resumido a lo esencial en la búsqueda de "the big picture". De este modo quién coleccione estos 2 volúmenes tendrá un excelente libro de seguridad informática

2. el contenido lo hemos dividido en 4 secciones: Fundamentos de Seguridad Informática, Ethical Hacking Paso a Paso, Seguridad Wireless y Herramientas. De este modo en "Fundamentos de Seguridad", aprendemos lo básico, la teoría. En "Herramientas", destacamos aquellas que no puede dejar de conocer un experto en IT. "Ethical Hacking Paso a Paso" nos muestra a nuestro enemigo, sus tácticas y cómo las aplica al momento de intentar comprometer nuestras redes. "Seguridad Wireless" es tan novedoso que necesariamente aparece en una sección separada.

Quienes hayan tenido contacto con NEX IT Specialist anteriormente encontrarán que algunos artículos ya aparecieron. La idea fue estructurar un libro coherente en los 2 volúmenes y para ello fue inevitable repetir algo del material.

Si a algún lector NO le interesara la Seguridad Informática (aunque lo dudamos) o desea aprender sobre algo distinto, al comienzo de esta edición encontrará 4 artículos de interés más general: "Moodle" (sinónimo de e-learning), "Weblogs y Syndication", el "buzz word" (palabras de moda) del mundo Web y un artículo sobreUtuto-e.

Finalmente inauguramos una nueva sección "Gente e Historia en IT". En esta oportunidad, brevemente introducimos a Andrew S. Tanenbaum y MINIX. Estamos seguros que les resultará de mucho interés.Este y varios artículos complementarios los encontrará en nuestros sitio web exclusivo para suscriptores.

Un último comentario sobre el título "Ethical Hacking": indistintamente podríamos haberlo llamado "Seguridad Informática" o "Las Mejores Herramientas del Experto en Seguridad Informática".



Revista de Networking y Programación

Año 3 - Número 13 - Edición Especial - Noviembre - Diciembre - 2004

Preimpresión e Impresión
Impresión: IPESA Magallanes 1315. Capital Federal. Tel 4303-2305/10
Impresión de esta Edición 8.000 ejemplares auditados por IPESA

Distrbución
Distribución en Capital Federal y Gran Buenos Aires: Distribuidora SANABRIA. Baigorri 103. Capital Federal. Tel 4304-3510
Distribuidora en Interior: Distribuidora Austral de Publicaciones S.A. Isabel la Católica 1371.
Capital Federal. Tel. 4301-0701

NEX - Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg3038

ISSN 1668-5423

Dirección: Av. Córdoba 657
Piso 12
C1054AAF - Capital Federal
Tel: +54 (11) 4312-7694
http://www.nexweb.com.ar

Indice de Contenidos NEX IT Specialist # 13













Ethical Hacking Volumen 1
Pag 15.



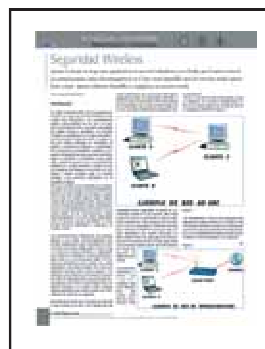
En Ethical Hacking Vol 1 y 2 presentamos una serie de artículos que conforman un verdadero libro sobre la seguridad informática con una propuesta diferente.

El contenido lo hemos dividido en 4 secciones:

Fundamentos de Seguridad Informática
Ethical Hacking Paso a Paso
Seguridad Wireless
Herramientas.

En esta edición le presentamos el Volumen 1.

Seguridad Wireless Pag 52.



Es tan novedoso que necesariamente aparece en una sección separada: abarca 3 artículos: "Seguridad Wireless", "Wireless Hacking" y "802.11Seguridad".

Fundamentos de Seguridad Informática.
Pag 16.

Aquí aprendemos lo básico, la teoría. Está compuesto de una serie de artículos que irán barriendo las diferentes temáticas sobre las que se basa la seguridad informática: Introducción a la Arquitectura Cliente-servidor, Entendiendo TCP/IP, "Elementos Basicos de Criptografía", "¿Algoritmos de Hash Seguros? y "Pass Phrases vs Passwords (parte 1 de 3)".

Ethical Hacking Paso a Paso
Pag 30.

Nos muestra a nuestro enemigo, sus tácticas y cómo las aplica al momento de intentar comprometer nuestras redes: "Introducción", "Footprinting", "Scanning", "Enumeración", Hacking Windows NT, W2K y W2003 (parte 1)" y "Alguien ha hackeado sistema operativo Windows,

¿Ahora Qué?"

TOOLS (herramientas)
Pag 64.

Describiremos las mejores herramientas de la seguridad informática: "NMAP y las 75 Mejores Herramientas de Seguridad Informática", "SNORT el NIDS (Network intrusión Detection System) bajo Windows", "Snort para Linux", NESSUS: el scanner de vulnerabilidades OPen Source" y "KNOPPIX y Distribuciones Especializadas en Seguridad bajo Linux.".



CaFeLUG

Los días 12 y 13 de Noviembre, se llevó a cabo en Bs. As. la "3ra Conferencia Abierta de GNU/Linux y Software Libre". Concurrieron aproximadamente 1300 personas (de 1800 registradas previamente). Se dictaron 61 conferencias / talleres con 7 salas en simultáneo, durante los 2 días. Participaron 42 disertantes e importantes miembros de la Comunidad de Software Libre local y de países vecinos.
La repercusión obtenida garantiza la repetición de este evento el año siguiente.
Dentro de los asistentes a la conferencia se contó con participantes de México, Uruguay, Chile y Bolivia.

Las siguientes entidades auspiciaron el evento:

UADE (Universidad Argentina de la Empresa)
USUARIA (Asociación Argentina de Usuarios de Informática y Comunicaciones)
GLEDUCAR (Construcción Cooperativa de Conocimientos , Software Libre en Educación)
LUGUM (Grupo de Usuarios de GNU/Linux , Universidad de La Matanza)
LANUX (Grupo de Usuarios GNU/Linux , ciudad de Lanús)

Medios Gráficos :

Revista Nex IT Specialist (Argentina)
Revista Users Linux (Argentina)
Revista Clarín Informática (Argentina)
Revista Mundo Linux (España)
Dominio Digital (Argentina)

Empresas:
Cor-Technologies , Xtech, Pixart , Open Computacion

Grupos de usuarios y organizaciones :
GrULIC, LANUX, LUGFI, LUGLi, LUGRo, RetroNet, SoLAr, UYLUG, Via Libre.





MOODLE

La herramienta Open-Source para la administración de la enseñanza.
www.moodle.org

Existe una enorme demanda para la educación a distancia. Esta necesidad se basa en factores especiales de la vida cotidiana en donde se mezclan responsabilidades laborales y compromisos familiares.

La competitividad del mercado laboral lleva a la necesidad de un mayor entrenamiento como herramienta para acceder a un mejor empleo. Se hace imprescindible por ello contar con un fácil acceso a la educación y perfeccionamiento.

Una herramienta para la administración de enseñanza (en inglés se dice learning management system o LMS) es un sistema de software que da las herramientas necesarias para proveer educación on-line.

Es decir, utilizando computadoras en red ya sean en "intranets" o accediendo a "Internet". Se utilizan principalmente en universidades, escuelas, instituciones de entrenamiento y empresas con el propósito de acercar conocimientos.

Las herramientas para la administración de enseñanza hacen uso extenso de la red incluyendo foros de discusión, chats, información en revistas de estudio (journals), sistemas de evaluación automatizados, herramientas de nivelación y seguimiento de los alumnos . Pueden emplearse también para enriquecer la enseñanza tradicional.

Los costos de educar on-line han sido siempre altos. Existen soluciones de software propietario de mucho prestigio como



¿Por qúe se llama MOODLE?

La palabra MOODLE, originalmente fue un anacronismo para Modular Object-Oriented Dynamic Learning Environment… Es también un verbo que describe el proceso de abordar algo en forma desganada, haciendo cosas a medida que se nos ocurra, una manera de moldear disfrutando y que muchas veces condice a profundizar y crear.

el Blackboard y webCT.

El elevado costo de las soluciones propietarias unido a la necesidad de poder modificar el software con el propósito de atender necesidades específicas de enseñanza y aprendizaje, hacen que sea necesario considerar con qué más se puede contar.

Existen varias herramientas open source. En este artículo presentaremos a MOODLE que reúne muchos de los requerimientos necesarios. Además, es una herramienta open source popular.

MOODLE comenzó en Australia en 1999 por el entonces estudiante de doctorado en Educación , Martin Dougaimas . Había sido formado en ciencias computacionales y no le satisfacían completamente las alternativas propietarias.

Moodle, desde entonces, se desarrolló muy velozmente con el empuje de su creador y gracias a una gran comunidad de usuarios y desarrolladores.

Un sitio Web bajo MOODLE puede administrar un gran número de cursos. Además existen gran variedad de posibilidades : los cursos por ejemplo pueden estar dirigidos por uno o varios maestros, se pueden realizar actividades múltiples como asignaciones, chats, seminarios, foros de discusión, revistas de estudio y planteamiento de problemática a resolver. Aporta también la posibilidad de asignar puntajes, el logging and tracking del usuario, el empleo de multimedios, integración de mails, entre otras posibilidades que lo hacen similar a las herramientas propietarias.

MOODLE se desarrolla sobre la plataforma LAMP, GNU/LINUX, APACHE, MySQL y PHP. Una característica muy interesante es que puede usarse sobre cualquier servidor que pueda correr PHP. Además puede emplearse PostgreSQL en vez de MySQL. Puede usarse incluso en servidores de hosteadores de sitios web. MOODLE se ofrece bajo la GPL de GNU (Licencia



Pública General).

Es muy fácil utilizar MOODLE e integrarlo con otros programas Open Source. Lo único que requiere el "alumno" es tener un browser (IE, Mozilla, Firefox…) y una conexión a Internet.

La gran mayoría de los LMS están centrados en el instructor y en cómo se desarrollan los contenidos de la clase.

Una particularidad interesante de MOODLE es que está basado en una filosofía orientada hacia el aprendizaje llamada pedagogía construccionista social.

¿Qué es LAMP?

Resume a Linux, Apache, MySQL y PHP. Es una plataforma open-source para desarrollo Web. Utiliza Linux como sistema operativo, Apache como servidor Web, MySQL como base de datos y PHP como lenguaje de scripting tipo object-oriented. Perl o Python sustituyen muchas veces a PHP. LAMP se ha transformado en un estándar de desarrollo de facto.
Vea el sitio web de O´Reilly: www.onlamp.com

En ella los estudiantes se involucran en su propio conocimiento.
El concepto de esta filosofía de aprendizaje es que los maestros construyen activamente nueva sabiduría, aprendiendo más y mejor al explicar el conocimiento a otros. Además adquieren así una perspectiva más subjetiva del conocimiento que han creado.

Este ideal corre en forma paralela a la forma en la que se han desarrollado los trabajos Open Source.
Los desarrolladores son también usuarios. Cada uno se encuentra libre para hacer su aporte al software y el código se va construyendo desde múltiples puntos de vista y se redefine a través de una discusión abierta.

Esta filosofía es la base del nombre especial del proyecto.

El sitio de la red MOODLE explica el origen del nombre siendo un acrónimo para un ambiente de enseñanza en módulos, dinámico y orientado hacia el objeto (en inglés Modular Object – Orientated Dinamic Learning Environment)

Las metas del proyecto MOODLE.

Estas se encuentran descriptas en el Moodle Developers Manual (Manual de Desarrolladores):

-Fácil de instalar, aprender y modificar.

-Corre en múltiples plataformas.

-Fácil de ascender de una versión a la siguiente.

-Permite la utilización en conjunto con otros sistemas.

-Al ser modular permite el crecimiento.



El tipo de pedagogía está reflejado en el diseño y elección de las características de MOODLE. Por ejemplo en cada curso hay un glosario de terminología. En el glosario los participantes del curso pueden agregar sus propios términos y definiciones.

Sinónimos de LMS

>> entorno educativo administrado

>> entorno de educación virtual

>> sistema de administración de cursos

>> sistema de soporte educativo

Además por ejemplo MOODLE permite que se adjunten comentarios de cada término permitiendo a los participantes redefinir y aclarar esas definiciones.

MOODLE es muy popular, se usa en cientos de países y muchos idiomas. Logra reunir características especiales que lo hacen apto para la cada día mayor demanda de educación a distancia.
A pesar de evolucionar rápidamente MOODLE se ha mantenido fiel a sus objetivos. Su última implementación es un calendario integrado.

Uno de sus aspectos más criticados es que se trata de un software únicamente para expertos en tecnología informática, ya que es dificultoso de instalar y utilizar para usuarios básicos.



Una encuesta realizada entre usuarios de MOODLE identificó que 66% de ellos se trataba de maestros, investigadores de e-learning o administradores educacionales.

Un producto LMS puede ser complejo. MOODLE simplifica muchas de las tareas. Pero, quizás lo mas rico es la comunidad que ha crecido alrededor de él.

Weblogs y Syndication

Uno puede suscribirse en este servicio de syndication en las páginas web y recibir alertas cuando han cambiado los contenidos. Se dice (en la jerga) que la página web produce un “feed” (alimentación) ante un cambio.

Por Núria Prats i Pujol

Apareció el WWW…(World Wide Web, 1990)
Hace unos años personas como (Sir)Tim Berners-Lee (el creador del HTTP, ver artículo en esta edición: “Gente e historia en IT”) mantenían páginas web con listas que promocionaban las nuevas e incluían pequeñas descripciones de las mismas. Sin embargo rápidamente estas “guías de páginas webs” se hicieron imposibles de mantener ya que diariamente se creaban miles nuevas.

Aparecieron los buscadores… (Yahoo, 1994, Google, 1998…(ver artículo en esta edición: “Gente e historia en IT”).
Normalmente uno realizaba una búsqueda. Encontrado algún sitio web de interés se lo incorporaba como “favorito o bookmark” en el web browser (IE, Netscape, Mozilla (Firefox aún no existía)…).
Pero, muchas páginas web se modifican con bastante frecuencia. Especialmente la de periódicos, sitios de noticias, revistas y otras.

Entonces uno hacía una especie de “syndication” (ver nota adjunta) manualmente. ¿Qué es esto? Luego de tener marcada la página web como favorito uno la accede diariamente y a veces más veces al día de modo de ver si hay cambios (novedades).

Aparecieron los weblogs… (páginas web, personales con comentarios y links, actualizadas sin ninguna sistemática o frecuencia). (leer sobre la historia de weblogs en: http://www.rebeccablood.net/essays/weblog_history.html

El mercado de la información actualizada como noticias de comercio, portales de periódicos y weblogs fue creciendo rápidamente.

El interés de poseer la información más actualizada se convirtió en un una necesidad y en un gusto. ¿Quién no ha renovado varias veces en un día ciertas páginas webs con la intención de ver si habían sido modificadas?
Syndication y weblogs son palabras que van de la mano. Introduciremos brevemente el concepto de weblog para profundizar luego en el sentido de syndication. Finalmente analizaremos la situación actual del tema.

Weblogs

Alrededor de 1997 comenzaron a aparecer diarios personales como páginas webs. En estos se publicaban noticias y resúmenes sobre diferentes temas que el autor consideraba relevante aportando además links de utilidad ligados a la temática discutida. Pero la forma de realizar y mantener la página era muy complicada. Se debía programar en html el formato de la página y cada vez que se quería introducir una modificación a la misma se debía crear un nuevo documento y ftp-earlo al servidor. Luego surgió la necesidad por parte de los lectores de interactuar con los editores de los weblogs. Comenzaron mediante consultas y respuestas por e-mail. Un modo muy complicado, especialmente si el editor-autor debía además refrescar la página con los comentarios de sus “lectores”.

Como respuesta a estas necesidades surgieron diferentes aplicaciones que permitían crear páginas web con formatos especiales para estas publicaciones personales. La forma de introducir las modificaciones era ahora muy sencilla y los lectores podían en forma simple hacer sus comentarios. Estas páginas especiales son los weblogs o blogs que es su diminutivo.

Las notas, artículos o noticias que el blogger (así se llama en la jerga al administrador-editor o autor del blog) desea publicar, se introducen rellenando una casilla como la que brindan actualmente los servidores de web-mail, señalando el tema o título (esto se llama un post o entry (entrada)).

Una característica esencial es que las distintas publicaciones posteadas en “los nuevos diarios personales” aparecen cronológicamente con fecha y hora y se pueden renovar, gracias a la simplicidad, varias veces al día. ¡La novedad es que se logra también la interacción con los lectores! Uno puede publicar comentarios o consultas debajo del artículo del blogger.
El número de weblogs que existen actualmente es inmenso (entre 2 y 4 millones) y en muchos se hacen varias publicaciones diarias. Si uno está acostumbrado a seguir algún weblog es muy probable que le interese también seguir el de alguna otra persona relacionada con este. Seguir las actualizaciones de diferentes weblogs se ha hecho cada vez mas complicado. Recordemos que además periódicos y revistas también modifican su contenido con asiduidad. La aparición de syndications (en cualquiera de los 2 formatos RSS o Atom) ha simplificado la labor de los lectores, ya que automáticamente les es reportado si se producen modificaciones en los weblogs que le interesen. Por ello, weblogs y syndication van siempre de la mano. O eso es al menos lo que los bloggers dicen.

Syndication

Dijimos anteriormente que uno podría hacer algo similar a syndication manualmente. En la actualidad esto está automatizado. De hecho es un servicio que ofrecen muchas páginas webs (especialmente de noticias) y weblogs.

Uno puede suscribirse a este servicio en las páginas web y recibir alertas cuando han cambiado los contenidos. Se dice (en la jerga) que el weblog produce un “feed” (alimentación) ante un cambio.

Los beneficios son varios ya que el alerta hará que uno sólo tenga que actualizar páginas únicamente cuando ha sido renovado su contenido y le sea de interés verla. Es que en la mayoría de alertas aparecen

Nota: RDF

Proviene de Resource Development Framework y es un recurso standard de desarrollos de syndication que utiliza XML. Es parte de W3C (World Wide Web Consortium) que guía los desarrollos de la web en el plano legal, social y comercial e intenta hacer la web accesible a todos los usuarios. [6]

los títulos y un breve extracto de los temas renovados. Así uno podrá seguir alguna noticia que se está desarrollando momento a momento, los resultados de un partido de football, el valor de ciertas acciones, o las novedades que ha publicado el blogger que uno sigue.

RSS 1.0 desarrollado por un grupo de O´Reilly (www.oreilly.com) (no es un upgrade de la versión de Dave Winer como se puede llegar a pensar, sino que tiene un formato original). RSS 1.0 usa RDF (ver nota) producido por el W3C(World Web Consortium).

Entendiendo qué es "Syndication"

En el mundo de los periódicos o diarios un "syndicate" distribuye información a los suscriptores (en este caso revistas o diarios), permitiendo que cada publicación use (si lo desea) los contenidos de la información que recibió. Tiras cómicas, noticias y columnas de opinión son distribuídas por "syndicates" dando más exposición a los autores y más contenido a los lectores. Desde hace pocos años, los desarrolladores de páginas web comenzaron a usar el término "syndicate" como verbo o sustantivo.

RSS son las siglas de Real Simple Syndication que es el formato más conocido sobre el que se programa la automatización de este servicio."To Syndicate" significa exactamente distribuir y creo que queda clara su utilidad.

Pero existe otra cara de esto que es que a las compañías de noticias les resuelve en parte los problemas de tráfico que ralentizan sus páginas cuando hay un acceso masivo a las mismas. A su vez, promocionan su compañía o weblog ¡directamente al público que lo desea!
Pero el potencial ha aumentado ya que hoy en día hay programas llamados aggregators de noticias que absorben los archivos RSS o Atom (feeds) y presentan las novedades organizadas en diferentes formatos. Estos programas permiten seguir la actualización de varias páginas a la vez. Algunos ejemplos: Feedreader, Feeddemon o Bloglines.

Historia de la evolución de RSS

1999 un año clave: nace RSS 0.90. Fue lanzado por Netscape con intención de ser un programa que facilitara el intercambio de datos entre páginas Web (de e-commerce y noticias principalmente). De esta forma se podía inscribir un usuario creando su propio canal en My Netscape. Al ser renovada la información de las páginas seleccionadas les seria automáticamente enviado a estos un resumen del cambio (un feed) [2].

Dave Winer, en ese entonces en la compañía UserLand Software, es quien introduce el Standard que finalmente evoluciona a la versión RSS 0.91 a la par que el grupo de Netscape desaparece. Así continúa la carrera de los RSS 0.9x.

Como alternativa a RSS 0.91 aparece

Los RSS 0.9x al día de hoy han evolucionado a la versión RSS 2.0. Dave Winer cedió sus derechos a la Universidad de Harvard. Este continúa participando del proyecto en el Berkman Center for Internet & Society at Harvard Law School. RSS 2.0

Diferencias entre Wikis y Weblogs.

Wiki es un Sitio-Web hecho en colaboración. Se forma por el trabajo continuo de muchos autores. Es similar a un WEBLOG en estructura y lógica. Un wiki le permite a cualquiera editar, deletear o modificar los contenidos que han sido publicados en el Sitio-Web. Aún el trabajo de autores previos. Para esto utilizara una browser (IE, Mozilla,…). A diferencia, un Blog es tipicamente manejado por un autor y no se permite que otros lo modifiquen. Solo se podrán adicionar comentarios al contenido original.

El término wiki se refiere indistintamente al Sitio-Web o al software que crea el sitio.

"Wiki wiki" significa "rápido"("quick") en Hawaiano. El primer Wiki fue creado por Ward Cunnigham en 1995.

posee una licencia "creative commons" que liberaliza los tan controversiales derechos del copyright.[1]

Paralelamente a las dos familias de formatos RSS (RSS 0.9x-RSS2.0 y RSS 1.0), aparece Atom. Este proyecto ha surgido por quejas que se realizaban a RSS y al hecho de que los derechos sobre código habían sido y eran de una única compañía. Atom es un open source software. [3]

Syndication: RSS vs. Atom

Hoy en día podríamos decir que existe una competencia entre dos tipos de syndication: RSS y Atom. Quizás el estallido de esta rivalidad surgió cuando Google (uno de los portales mas visitados de la www) anunció que ofrecería solo Atom syndication a sus usuarios bloggers. Algunos sitios que utilizan RSS son por ejemplo la BBC, CNN, Disney y Forbes entre otras.[5]

Atom es un intento de resolver muchos de los problemas asociados con RSS. Sus desarrolladores hicieron de la internacionalización una prioridad. De este modo Atom puede producir "Syndication Feeds" en cualquier idioma. También se buscó introducir extensiones: que sea posible sumar funcionalidades sin tener que redefinir las especificaciones base de Atom.
RSS se diseñó para resumir un Feed. Atom se creó con un propósito más general. Por ejemplo es posible usarlo en bibliotecas donde se podrán producir feeds de Atom de las últimas adquisiciones o máquinas en una fábrica producirán reportes sobre su estado en Atom. Programas tipo "aggregators" leerán los feeds mostrando los nuevos libros o que máquinas no funcionan correctamente (ver [4])

Estos objetivos diferentes han hecho que los dos proyectos vayan en paralelo y es muy difícil predecir cual será el futuro en syndication. Solo el uso y el tiempo marcarán el camino.

Bibliografía:

[1]http://blogs.law.harvard.edu/tech/rssVersionHistory
[2]http://www.internetnews.com/bus-news/article.php/3_80051
[3]http://news.zdnet.com/2100-3513_22-5157662.html
[4]http://www.xml.com/pub/a/2002/12/18/dive-into-xml.html
[5]http://www.webreference.com/authoring/languages/xml/rss/intro/
[6]http://www.w3.org/Consortium/#goals

Para recomendar

Rebeca Blood www.rebecablood.net

Nota en PC Users #163 pag60, 2004 por Jorge Gobbi.

Quiero tener mi Blog !!!!!!!!!!!!!!

>>Lo más simple.
El proceso es similar que con el webmail. Alguien me provee un "weblog server" que hosteará mi blog y una interfase gráfica donde editaré y postearé mi contenido.
Ejemplos: www.blogger.com; blogs.ya (Pitas, Diaryland)

>>Si deseo una infrestructura más profesional.
Puedo utilizar Word Press (WP) o Movible Type (MT). Aquí debo poseer un hosting propio que acepte Perl y CGI para MT o PHP y MySQL para WP. El procedimiento es aún sencillo pero más involucrado. Pero, da más funcionalidades mediante el uso de plug-ins.

>> No estoy on-line
Creo todo mi blog sobre mi PC sin estar conectado a internet (no estoy on-line). Luego lo subo (ftp-eo) a mi web-site.

Ejemplos: http://thingamablog.sourceforge.net ; www.wbloggar.com

>>Tengo un servidor Apache y quiero usar aplicaciones del mundo open-source para hostear weblogs.
Instalo Blosxom o CORE (ver NEX IT Specialist #10 pag 3)

Hacer nuestro BLOG es tan fácil como hacer 1, 2, 3.

en www.blogger.com (su dueño actual es Google Inc.)

Núria Prats i Pujol

Es consultora en programación web/base de datos. En la actualidad realiza su doctorado en Física Teórica en la Universidad de Barcelona, España.

Se la puede contactar en:
nuriapip@nexweb.com.ar



UTUTO-e: la primera distribución GNU/Linux argentina y 100%

La evolución de UTUTO ha dado como resultado en nuestros días a UTUTO-e, una distribución GNU/Linux destinada exclusivamente al uso como escritorio, lista para ser instalada en el disco rígido y conformada únicamente por software libre

Autor: Dr. Reinaldo Piz Diez

Hacia fines del año 2000 el ingeniero Diego Saravia, de la Universidad Nacional de Salta, presentó en sociedad la primera distribución GNU/Linux argentina, UTUTO. Dos características permitían sobresalir a este producto. En primer lugar, un único CD contenía los paquetes necesarios para tener una distribución funcional, escritorio incluido, en poco tiempo. En segundo lugar, el CD era de modalidad liveCD, es decir instala la distribución en memoria temporalmente y sin afectar el o los sistemas operativos ya instalados en el disco rígido.

La evolución de UTUTO ha dado como resultado en nuestros días a UTUTO-e, una distribución GNU/Linux destinada exclusivamente al uso como escritorio, lista para ser instalada en el disco rígido y conformada únicamente por software libre, como no se cansan de enfatizar sus autores, Daniel Olivera y Pablo de Nápoli, integrantes junto a Saravia de SOLAR, Software Libre Argentina [1].

El proyecto UTUTO-e tiene en la actualidad su propia página web, https://e.ututo.org.ar/indexes.html. Desde ella es posible acceder a la página de descarga de la distribución. La primera sorpresa es que podemos elegir qué descargar en función del tipo de procesador de nuestra máquina. En particular, podemos elegir entre los tipos 486, III y IV de procesadores Pentium y Athlon y Duron de la familia AMD. En el caso de procesadores Pentium es posible descargar la versión 686, válida para procesadores 486, III y IV. Dado que las pruebas que se comentan en este artículo se realizaron sobre una PC con procesador Celeron de 1.8 Ghz, se descargó la versión 686 [2].

Figura 1. El escritorio de Ututo

Al reiniciar la PC con el CD de la distribución, las primeras pantallas recuerdan mucho a las pantallas de inicio de la distribución GENTOO [3]. Luego de cargar una imagen del kernel 2.6.6 y reconocer automáticamente el hardware básico de la PC, se nos pide seleccionar el idioma a usar durante la instalación entre tres posibilidades: inglés, español y portugués.

El próximo paso es el Menú de Instalación en el cual nos encontramos con dos posibilidades: instalación automática o instalación manual. Elegimos la segunda opción. La primera operación es la partición del disco rígido para lo cual se utiliza cfdisk v2.12. Creamos sólo dos particiones, la región swap en /dev/hda1, con un tamaño de 256 MB (la memoria de nuestra PC es de sólo 128 MB), y /dev/hda2 para /, con el resto del disco rígido y capacidad de arranque. Optamos por escribir la tabla de particiones.

Luego de haber creado las particiones, se nos ofrece crear y / o configurar el gestor de arranque de la PC, para lo cual se muestra en pantalla el archivo lilo.conf. Dado que el mismo no presenta opciones extrañas, lo salvamos sin modificarlo.

El siguiente paso es el formateo de las particiones elegidas anteriormente utilizando mke2fs. Inmediatamente después del formateo, se instalan en el disco rígido los archivos correspondientes al kernel y al sistema base. Posteriormente, se copian archivos del CD al disco rígido y comienza la instalación de los respectivos paquetes, 377 en total.

Una vez finalizada la instalación de los paquetes, es posible seleccionar el tipo de teclado y el lenguaje,

generar la clave para el administrador, escoger los servicios que se activarán durante el arranque, configurar el acceso a internet o una red interna con la posibilidad de activar samba si se forma parte de una red Windows y crear cuentas de usuarios. Finalmente, la configuración del entorno gráfico se realiza automáticamente.

¡Listo! Ya estamos en condiciones de reiniciar la máquina. Al hacerlo se nos permite elegir entre un kernel 2.4.25 y uno 2.6.6. Al ingresar en la cuenta de administrador nos encontramos que por alguna razón la configuración automática del entorno gráfico falló, razón por la cual ingresamos al sistema en modo consola. No obstante, UTUTO-e tiene un excelente menú de configuración post-instalación en /admin/menu. Desde allí configuramos manualmente el entorno gráfico para una tarjeta SIS650 y luego de ejecutar "startx" nos encontramos con un escritorio GNOME con un papel tapiz con la pequeña lagartija que le presta su nombre al proyecto, ver figura 1. Para mi sorpresa, la

Figura 2. Planilla de cálculos Gnumeric

tarjeta de sonido tipo Intel810, empotrada en una placa madre no Intel, fue configurada automáticamente y con éxito por el sistema ALSA [4].

Veamos ahora una resumida lista de los programas y utilidades disponibles en UTUTO-e:

Procesador de textos Abiword.

Planilla de cálculos Gnumeric, ver figura 2.

Cliente de Correo Sylpheed, ver figura 3.

Navegador de Internet Firefox, ver figura 4.

Suite Ofimática KOFFICE (Procesador de textos, Planilla de cálculos, generador de presentaciones, gratificador de vectores, generador de reportes profesionales, generador de "charts", editor de formulas, generador de "flowcharting" estilo Visio), ver figura 5.

Grabador de CD y DVD K3B, ver figura 6.

Reproductor de CD.

Reproductor de archivos de música.

Sistema de impresión CUPS.

Sistema de Sonido ALSA.

Manejo de protocolos de comunicación de Windows (SAMBA).

Sistema de administración remota mediante WEBMIN.

Sistema de reconocimiento automático de hardware.

Sistema de "hotpluging" para dispositivos PCI y USB.

Configuración automática del servidor gráfico X.

Soporte de protocolos de Internet IPv4 e IPv6 integrados en todas sus aplicaciones.

Kernel con soporte SMP hasta 8 procesadores.

Firewall basado en iptables y ncurses FIREWALL-JAY.

Reproductor multimedia MPLAYER.

MPLAYER "plug in" integrado en el navegador de Internet.

Paquete para edición y manejos de gráficos GIMP 2.0.

Sistema de edición de diagramas DIA.

Sistema de acceso telefónico a redes PPP.

Manejador de conexiones ppp

Figura 3. Cliente de Correo Sylpheed






Figura 1. Navegador de Internet Firefox

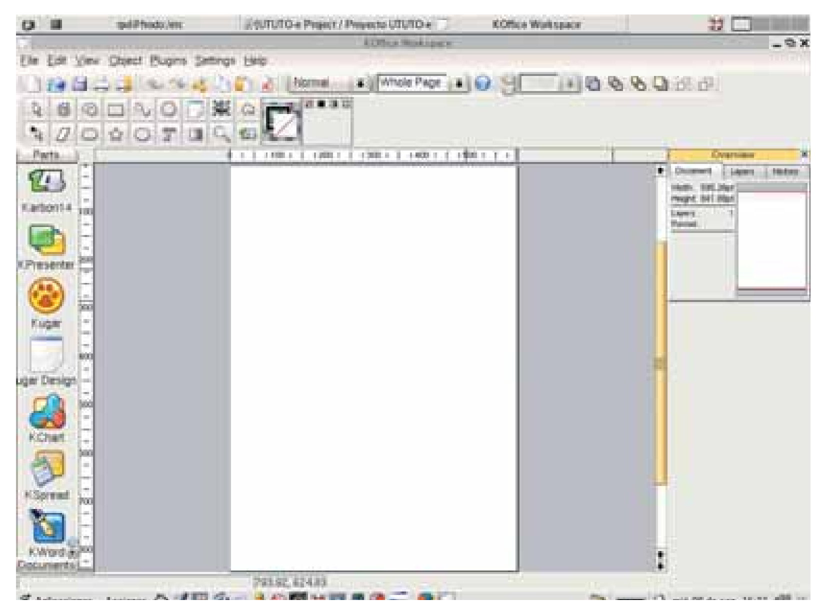

Figura 5. Suite Ofimática KOFFICE


Figura 6. Grabador de CD y DVD K3B

WVDIAL.

Manejador de tablas de particiones QTPARTED.

Manejador de paquetes fuentes Portage de Gentoo.

Se desprende claramente de esta lista que se dispone prácticamente de todas las herramientas necesarias para desarrollar tareas de escritorio u oficina, aunque el entorno se adapta perfectamente también a los requerimientos de un programador. Dado que los paquetes han sido optimizados para cada arquitectura, el rendimiento es el óptimo aunque no debemos olvidar que los entornos gráficos, aun en Linux, consumen apreciables recursos de memoria.

Es importante dejar en claro que la ausencia de algunos paquetes muy conocidos, como el suite de oficina OpenOffice, no implica que no puedan utilizarse. Simplemente, su política de distribución no es compatible con la filosofía de los desarrolladores de UTUTO-e y por lo tanto el paquete no es incluido en el CD. El usuario final es libre, no obstante, de descargarlo e instalarlo.

Para finalizar este artículo, digamos que UTUTO-e, la primera distribución GNU/Linux argentina y conformada totalmente por software absolutamente gratis, es un producto de excelente calidad, sin nada que envidiar a distribuciones con más tiempo en el mundo del Linux. Además, la distribución completa esta contenida en un único CD, a diferencia de otras distribuciones “tradicionales”. Finalmente, UTUTO-e tiene el orgullo de ser una de las pocas distribuciones recomendadas por la Free Software Foundation como Free Operating System [5]. Por todo esto, UTUTO-e merece ser considerado por los “linuxeros” argentinos como una fuerte opción para una configuración de escritorio.

Referencias y links de interés

[1] http://www.solar.org.ar.

[2] Las pruebas que se comentan fueron efectuadas con la versión 1.1 de UTUTO-e. Al momento de escribir este artículo se encuentra disponible la versión 1.2.

[3] http://www.gentoo.org.

[4] http://www.alsa-project.org/.

[5] Ver http://www.fsf.org/links/links.html#FreeGNULinuxDistributions.

```
<script language=Javascript>

Function somequotes(){
//Create an array
var quotes=new Array()

quotes[0]='HI'
quotes[1]='Always paraise dgfzdz'
quotes[3]='If (Exists(GOD)){MakeKumar=Mil
lionaire;}else{YouDonateMo
neyTo=Kumar;}'
quotes[4]='It is convenient That there be GOD'
quotes[5]='Some more quotes.'quotes[6]='Even <img src="imgsource/image.gif" border=0 alt="Display
 images randomly"> display
quotes[8]='You can also add layers'
quotes[9]='Bottom line is that you can use valid html with escape sequence'

var whichquote=Math.floor(Math.random()*(quotes.length));//which quote to display

var fontstylestart='<font face="MS San
var fontstyleend='</span></b></font>'
document.write(fontstylestart+quotes[whichquote]+fontstyleend)
}
//usage
//Put above function in the head.
//Call the function where you want quotes to be displayed
Function mov_it()
```

1. FUNDAMENTOS DE SEGURIDAD INFORMATICA

A. Introducción a la arquitectura Cliente Servidor
B. Entendiendo TCP/IP
C. 1 Elementos de Criptografía
C. 2 ¿Algoritmos de Hash seguros?
D. Pass Phrases vs Passwords (Parte 1 de 3)

2. ETHICAL HACKING PASO A PASO

Paso 0. Introducción
Paso 1. Footprinting
Paso 2. Scanning.
Paso 3. Enumeración
Paso 4. Hacking WINDOWS (Parte 1)
Paso 5. Alguien ha hackeado mi Sistema operativo

ETHICAL HACKING

Edición Especial - Volumen 1

3. SEGURIDAD WIRELESS

1. Seguridad Wireless
2. Wireless Hacking
3. 802.11Seguridad

4. TOOLS (herramientas)

1. NMAP y las 75 mejores herramientas de seguridad Informática
2. SNORT EL NIDS (Network Intrusion Detection System) bajo Windows
3. SNORT para Linux
4. NESSUS: El scanner de vulnerabilidades Open Source.
5. KNOPPIX y Distribuciones especializadas en Seguridad bajo Linux.

En Edición Especial Vol 2 continuaremos entre otros con los siguientes temas:

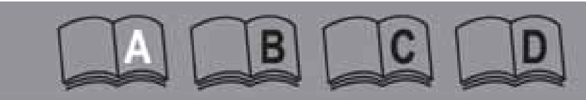
Ethical Hacking Paso a Paso

Paso 6 Hacking Windows (Parte 2)
Paso 7 Hacking Unix-like (UNIX, BSD, FreeBSD, Linux...)

Herramientas: NETCAT

Fundamentos de seguridad informática

Autenticaciones en Windows - SQL Injection - Virus y Gusanos
Etica y temas legales - Autenticación de 2 factoresSpoofing
Comunicaciones seguras (SSL, SSH, IPsec, VPNs (PPPTP, L2TP))
Troyanos y backdoors (puertas traseras)
Sniffers - Ingeniería social - Hijacking de Sesión
Hackeo de servidores web - Metodologías de Tests de Penetración



Introducción a la arquitectura cliente servidor

redes y la seguridad informática

En este artículo veremos un panorama general de los elementos básicos en los que se basan las redes de computadoras hoy. Muchas tecnologías entran en juego. En los artículos que siguen discutiremos detalles de cada una de ellas.

1. ¿Qué beneficio obtenemos en tener una red?

Respuesta: tener máquinas en red nos ayuda a resolver un gran número de problemas.
El fin último de cualquier proyecto de redes es la de proveer algún tipo de servicio en una o en un conjunto (caso de clusters) de máquinas que será utilizado por usuarios desde otras máquinas de la red. Ejemplos:
-Necesito ver la página web de Ovis Link para conocer los precios de routers, hubs, switches, productos wireless. Existe un Web Server que aloja las páginas del dominio ovislink.com
-Necesito enviar un e-mail. Deberá existir un mail server y deberé ejecutar una aplicación cliente que me envíe y reciba una posible respuesta.
-Necesito compartir archivos y carpetas a toda mi empresa. Y que estén en un solo server (file server) de modo de centralizar los back-ups.
-Necesito comprar una flauta traversa de plata: www.ebay.com y tipear ¨traverse flutes¨.

2. ¿Cuáles son los elementos fundamentales en una red ?

A. Todo tipo de servicio de red necesita un server-software y un client-software.
Relación ¨cliente servidor¨ entre máquinas.

Conectamos las máquinas en red con un propósito: la computadora que actúa como cliente se beneficia de las computadoras que actúan como servidores (ver fig. 1)
-En la maquina cliente debe correr un programa que sepa solicitar un servicio y saber como recibir y mostrar lo que recibió: "aplicación cliente".
-Necesito en el servidor un programa que esté atento y sepa escuchar pedidos y enviar la información solicitada: "aplicación servidor"
Un ejemplo muy popular es el de Web browser (cliente) - web server (servidor):
Si quiero ver la página web del periódico NEX utilizo mi "web-browser" (cliente web) y en algún lugar tipeo: http://www.nexweb.com.ar (http hipertext transfer protocol, es el protocolo que permite transferir hipertexto).
He dicho a la red: "quiero la página web de nexweb.com.ar que está alojada en algún servidor llamado www". En nuestro caso no está en las oficinas de NEX sino en un proveedor de web-hosting (towebs).
Los paquetes saben encontrar donde está el servidor. ¿Cómo?
Se lo preguntan al servidor DNS: ¿"cuál es el número IP del servidor (llamado www) que aloja la página web de nexweb.com.ar". DNS devuelve el IP correcto y los paquetes con el pedido viajan hasta la máquina con ese IP. El web-server (servidor) que está constantemente "escuchando" (tiene corriendo un pequeño programa llamado daemon, demonio). Toma el pedido y envía, por ejemplo, el archivo index.html. El cliente lee el html y me lo muestra en pantalla.

Otros tipos de servidores incluyen: file servers (servidores para compartir archivos), print servers, (servidores de impresión), E-Mail servers; Servers de Negocios online (E-commerce).

B. Las redes necesitan hardware para conectarse (switches, hubs, routers, modems) y conexiones (cables de red, líneas telefónicas, frame relay, DSL, cable modem, ISDN y otros). Sino, los clientes NO pueden conectarse a los servidores.

> Web-browsers más conocidos: Netscape, Mozilla, Internet Explorer, Firefox.
>
> Web-servers más conocidos: Apache (normalmente bajo Linux) e IIS (Internet Information Server) sólo trabaja bajo Windows.

En la figura 1 vemos un esquema sobresimplificado de una LAN (Local Area Network) con conexión a internet.
Por ejemplo la subnet (red) 192.168.57.0 se conecta con 192.168.60.0 a través de un router (Router 1) El router tiene dos interfases (una en cada subnet). Las máquinas de cada subnet están conectadas por un hub o switch. La conexión a internet la realiza el Router 2.

C. Los clientes y servidores deben hablar los mismos protocolos de red.
Las máquinas (sus sistemas operativos) deben hablar el mismo "idioma de red" (network transport protocol).

Han existido diversos protocolos de comunicación:
-NetBEUI (Network Basic Input /Output System Extended User Interfase)., un Viejo protocolo de Microsoft /IBM/ Sytex usado para soportar pequeñas redes).
-IPX / SPX (Internet Packet Exchange / Sequenced Packet Exchange), el protocolo que Novell NetWare utilizó durante muchos años.

> sistemas operativos más usados: UNIX, Windows, Linux, Novell

-TCP / IP (Transmition Control Protocol/ Internet Protocol), el protocolo casi universal utilizado hoy.

Si TCP/IP es nuestro protocolo de comunicación, utilizaremos ciertos servidores fundamentales para soportar su implementación:

-Servidor DNS (Domain Naming System) que conoce los nombres de las computadoras en la red y nos traduce a su numero IP.

-Servidor DHCP (Dynamic Host Configuration Protocol) nos ayuda a configurar las maquinas de nuestra red con su configuración IP.
-WINS (Windows Internet Name Service) hace algo parecido a DNS pero sobre los nombres NetBIOS de nuestras máquinas. Como NETBIOS es una interfase (API) de la implementación de redes Microsoft WINS NO será necesario en un entorno exclusivo UNIX.

D. Las redes necesitan seguridad.

Una vez establecidos los puntos a, b y c el trabajo ha concluido: puedo leer y escribir archivos en el file server, ver páginas web en el web server, imprimir en impresoras manejadas por el print server…

Pero ésta idea de compartir y de estar ofreciendo los servicios lleva implícita un peligro. Nos está faltando entender cómo me protejo de alguien que quiera aprovechar esta configuración para hacer un daño o robar información. La palabra seguridad aparece junto con dos conceptos fundamentales: autenticación y permisos.

1. Debo autenticar (verificar, identificar) a quien pretenda entrar a mi red y obtener un servicio.

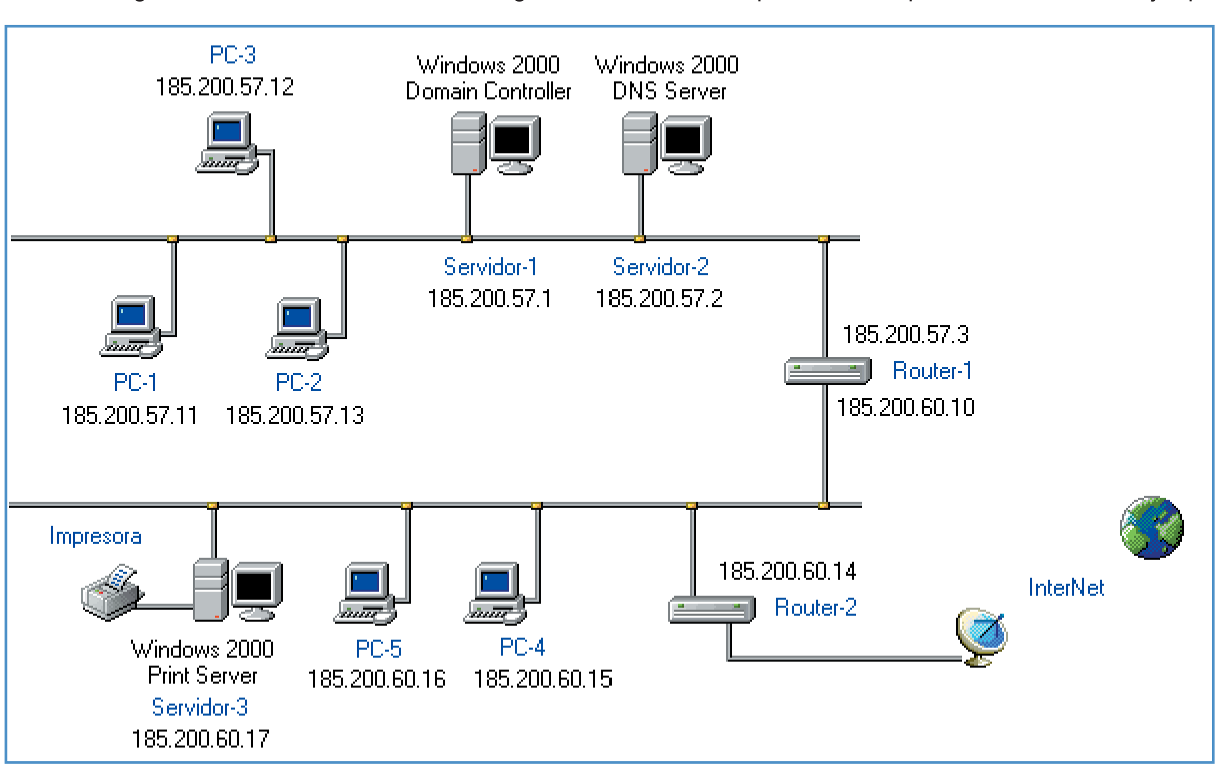
2. Una vez autenticado debo tener almacenado en algún lugar la información de "qué" tiene permitido hacer en la red. (sus permisos).

El punto 1 de seguridad llamado autenticación normalmente se logra con una "cuenta" (nombre de usuario, user id) y un password (contraseña). Hoy existen variantes más sofisticadas: smart cards y tecnologías biométricas (huellas digitales, cara, voz, retina).
Ahora debo guardar la información de usuarios y sus passwords en alguna base de datos centralizada y necesito "encriptar" esa información. Recordar que siempre existe la posibilidad de que alguien acceda o robe esa base de datos. Por ejemplo los servidores NT4 guardaban información de usuarios en un archivo llamado SAM. Aún cuando el archivo estaba encriptado un grupo de hackers logró saber cómo crackear la información. Hoy Windows 2000 y 2003, que se basan en dominios, usan un modo más sofisticado de encriptación cuya información también es posible descifrar (el archivo se llama NTDS.DIT en lugar de SAM). Aclaremos que el peligro esta si alguien accede físicamente a esos servidores (domain controlers, DC) donde se guardan las cuentas / passwords. Por eso normalmente esos servidores deberán estar a buen resguardo.
Síntesis: tenemos un servidor en algún lugar de la red con las cuentas y passwords. Por ejemplo la infraestructura que MS usa para organizar la red se llama Active Directory . Y el servidor con cuentas y passwords (Domain Controler) DC que lo podemos pensar como un servidor de logueo.
Ahora cualquiera que quiera acceder a los "beneficios" de la red se deberá sentar en alguna máquina y entrar user ID y password: logonearse.
Pero ahora surge un problema muy serio. Yo tipeo mi user ID y password y estos deberán viajar por la red para ser verificados en el DC. ¿Pero no existen programas llamados "sniffers" que pueden ver los paquetes que viajan por la red ? Sí. Por eso diferentes estrategias han sido y son utilizadas para realizar ésta acción de logonearme para poder acceder a algún recurso de red compartido sin comprometer el password.
Por ejemplo MS utilizó hasta los servidores NT un método de autenticación llamado NTLM (NT LAN MANAGER). Hoy en una red que use Active Directory se usará un viejo método del mundo UNIX (1980) llamado Kerberos.

Aparecen hoy otros modos de autenticarse como por ejemplo las llamadas "smart cards". Ellas utilizan una infraestructura diferente llamada PKI (Public Key Infrastructure) basada en certificados y dos claves (keys), una pública y otra privada
Aclaremos que hemos ejemplificado el proceso de autenticación al de una persona (usuario). Pero también deberán autenticarse las máquinas entre sí y los servicios. Las infraestructuras detalladas antes también serán usadas en estos casos.

El segundo punto son los Permisos y Access Control Lists (ACLs). Una vez autenticado la pregunta es a qué tiene derecho dentro de la red. Eso se gobierna con una infraestructura de permisos también llamados derechos y privilegios. Ejemplos:
-El file server de la empresa tiene 6 carpetas compartidas, pero el usuario "Pepe" sólo puede acceder (tiene permiso) para una sola. Y quizás el permiso sólo lo deje "read" (leer) los archivos pero no modificarlos.
-El usuario "administrador" tiene derecho a crear cuentas de usuarios.

Con lo anterior (autenticación y permisos) ejemplificamos uno de los temas que componen la seguridad en el mundo IT. Pero no son los únicos. Por ejemplo



- Cuando solicito información a un website o envío / recibo un e-mail, ¿cómo puedo hacer para que nadie vea los contenidos? La respuesta es encriptándola.

- ¿Cómo me aseguro de quién me envía un cierto e-mail? Respuesta: digital signing.

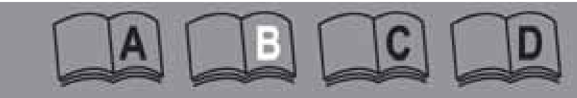
- ¿Cómo hago una compra segura con mi tarjeta de crédito via web? Normalmente aparece https y no http en el browser. La comunicación a partir de ahí se hará encriptada usando SSL (Secure Sockets Layer) que utiliza encriptación asimétrica de llaves pública y privada (PKI).

- ¿Porqué un hacker puede acceder a mi computadora utilizando las llamadas "vulnerabilidades"?

- ¿Qué significa que el programa .exe que llega como attachment en un e-mail me cree un back-door?

En los artículos de esta colección que siguen expondremos todos estos y otros conceptos que conforman la seguridad informatica (ingeniería social, hashes, virus, gusanos, troyano…).

(Para complementar este artículo los invitamos a ver una excelente presentación en video (de 12 minutos) donde se ejemplifica todo el proceso de uso de TCP / IP en redes). (download: www.warriorsofthe.net)



Entendiendo TCP/IP

Los fundamentos para comprender seguridad informática

TCP/IP es una suite (conjunto) de protocolos. Allí se incluye la información del número IP del que envía, del que recibe, el puerto de la aplicación que envía los datos, el puerto destino y toda otra información relevante a la comunicaci n.

Toda la información que viaja por Internet (y en redes en general) está contenida en "frames" (paquetes). Estos paquetes están conformados por los "datos" que una cierta aplicación quiere enviar (por ejemplo al hacer http://www.yahoo.com estoy enviando algo como: "dominio yahoo.com dame tu pagina web"). A éstos "datos" se le adicionan "headers" (encabezados) por los diferentes protocolos de TCP/IP. Lo malo, lo bueno, lo que quiere hacer mal, todo está dentro de los "frames".

TCP/IP es una suite (conjunto) de protocolos. Como ya dijimos, cada protocolo en un dado orden, agrega a los "datos" a ser enviados un "header". Allí se incluye la información del número IP del que envía, del que recibe, el puerto de la aplicación que envía los datos, el puerto destino y toda otra información relevante a la comunicación.

Quienes quieran realizar una maldad (hackers) o quienes desarrollen herramientas de protección (antiviruses, firewalls, proxys) deberán conocer a fondo el detalle de cómo están conformados los paquetes.
En este artículo se explicará ese detalle. Se verá una introducción histórica de TCP/IP, el modelo que lo describe, y un análisis de los headers que se agregan cuando se conforman los paquetes.
Si desea entender cualquier artículo sobre seguridad o implementar alguna herramienta será indispensable tener claro lo aquí expuesto. En otro artículo de esta colección estará dedicado a explicitar en detalle ampliado sobre los protocolos IP, TCP y UDP.

TCP/IP

Los protocolos TCP/IP (también llamados "Internet Protocols") son la "amalgama" que conecta hoy la mayoría de las redes de computadoras. También son responsables de la existencia de Internet: la red de redes que nos permiten entre otras cosas enviar correo electrónico, poder ver páginas Web y realizar transacciones comerciales en materia de segundos sin tener un límite geográfico. Los protocolos TCP/IP fueron originalmente desarrollados para tareas de investigación pero han logrado un alto grado de maduración y aceptación casi universal. Las investigaciones realizadas por el mundo académico fueron financiadas en su mayor parte con subsidios de las fuerzas armadas americanas, a través del proyecto ARPANET (Advanced Research Project for Networking. Año 1969).

En 1983 se divide en dos redes: MILNET (de uso militar) e INTERNET (de uso académico). En 1990 INTERNET se hace comercial y surge el boom del e-commerce e infinidad de otros mundos.
TCP/IP se refiere a un conjunto (suite) de protocolos para comunicación de datos. La suite toma su nombre de dos de los protocolos que lo conforman: Transmition Control Protocol (TCP) e Internet Protocol (IP).
La figura 1 nos detalla algunos de los protocolos más comunes que conforman la suite. (Figura 1)

TCP/IP Suite

Los protocolos asociados con TCP/IP incluyen los siguientes:

IP	Internet Protocol
TCP	Transmission Control Protocol
IGMP	Internet Group Management Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
RARP	Reverse Address Resolution Protocol
UDP	User Datagram Protocol
FTP	File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

Figura 1

Modelos para describir la arquitectura de comunicación de datos

Un modelo arquitectónico fue desarrollado por la International Standards Organization (ISO) y usado para describir la estructura y función de los protocolos de comunicación de datos: OSI (Open Systems Interconnect Referente Model). Ver Figura 2.

Arquitectura TCP/IP

Modelo OSI	Implementación TCP/IP
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data Link Layer	Network Interface Layer
Physical Layer	

Figura 2

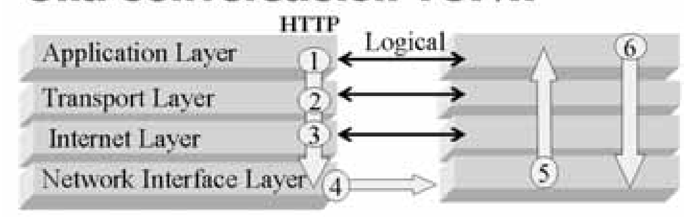
Contiene siete capas (layers) que definen las funciones de los protocolos de comunicación de datos. TCP/IP puede ser descrito con el modelo OSI pero existe un modelo de arquitectura (alternativo) propio (ver Figura 2, TCP/IP implementación) compuesto por cuatro capas.
Cada capa representa una función que se realiza en la transferencia de datos entre aplicaciones a través de la red. Se lo llama un "apilamiento" o "stack".

Una capa no define un solo protocolo. Define una función que puede ser realizada por un número de protocolos. Por ejemplo, un protocolo de transferencia de archivos (FTP) y uno de correo electrónico (SMTP) proveen servicios al usuario y son parte del Application layer.
Cuando dos máquinas se comunican, cada protocolo se comunica con su "peer" (par). Un par es una implementación del mismo protocolo en la capa equivalente en el sistema remoto.

En principio cada protocolo debería sólo interesarse de la comunicación con su peer. Sin embargo, deberá también haber un acuerdo de cómo pasar los datos entre capas dentro de una sola computadora. Los datos son pasados bajando por el "stack" de una capa a la otra hasta que es transmitida por los protocolos de la llamada "Physical Layer" por la red. Por otro lado los datos son tomados de la red y subidos a través del "stack" hasta la aplicación receptora.

Las capas individuales no necesitan saber cómo funcionan la capa superior e inferior a ella: solo como pasar los datos (ver Figura 3).

Una conversación TCP/IP



1. El layer de aplicación prepara un pedido HTTP.
2. TCP negocia el envío garantizado de los datos. Un header TCP es agregado al pedido en este layer.
3. El header IP, incluyendo la dirección IP de las computadoras remitente y destinataria, es agregado al paquete.
4. Las direcciones físicas para computadoras que envían y reciben son agregadas al paquete. La información es transmitida como señales de luz o electricidad a la otra computadora.
5. Cuando el paquete llega a la otra computadora, va en sentido reverso a traves de layers.
6. El servidor de Web , envía los datos solicitados utilizando el mismo proceso.

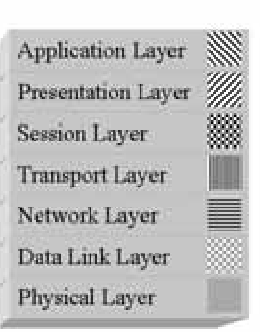
Figura 3

Este aislamiento de funciones en cada capa minimiza el impacto sobre toda la suite, que se puede producir por los avances tecnológicos.

En cada capa del "stack" se adiciona información de control llamado "header" (encabezado) ya que se coloca al frente de los datos a transmitir (ver Figura 4).

Cada capa trata toda la información que recibe de las capas superiores como "datos" y adiciona "su" propio "header" (proceso llamado encapsulación). Cuando se recibe información sucede lo opuesto.
Es importante resaltar que cada capa define una estructura de datos independiente de las otras y su propia terminología que la describe.

Headers



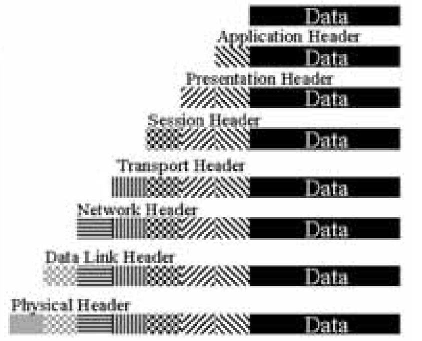


Figura 4

La Figura 5 muestra los términos usados en las diferentes capas para referirse a los datos transmitidos (ej.: un "datagrama" tiene el "header" correspondiente a la internet layer y lo que le pasa la capa superior).

Descripción de cada layer

Las figuras 6, 7 y 8 muestran una representación pictórica de la estructura de los "headers" y datos. "Los "headers" están conformados por varios "words" de 32 bits donde se incluye información. Recordar que cada layer tiene su propia estructura (Figura 4) y agrega un "header" a lo que recibe de la capa superior que lo toma como "datos". Esta información adicional que garantiza el "delivery"(entrega), como ya dijimos, se llama "encapsulación". Cuando se reciben "datos" lo opuesto sucede. Cada layer elimina su "header" antes de pasar los "datos" a la capa superior. Cuando la información sube el stack, lo que llega de la capa inferior es interpretada como header y datos.
La información de los estándares de los diferentes protocolos es desarrollada y publicada a través de los llamados "Request For Comments". (Ver nota)

Network Access (o Interface) Layer (Capa de Acceso a la red)

La Network Acess Layer es la de más abajo en la jerarquía de protocolos TCP/IP. Los protocolos en esta capa proveen el modo en que el sistema envía los datos a otros dispositivos en una red a la que está directamente conectado.

Layer	TCP	UDP
Application Layer	Stream	Message
Transport Layer	Segment	Packet
Internet Layer	Datagram	Datagram
Network Access Layer	Frame	frame

Figura 5

Si aparecen nuevas tecnologías de hardware deberán desarrollarse nuevos protocolos para la Network Acess Layer. Hay muchos protocolos de acceso: uno para cada Standard de red física. (Ethernet, Token Ring, Cobre-teléfono, Fibra.)
Las funciones que se realizan a este nivel incluyen encapsulación de datagramas IP ("frames" que se transmiten por la red) y el mapeo de números IP a las direcciones físicas usadas por la red (ej.: el MAC address).
Dos ejemplos de RFCs que definen protocolos de esta capa son:

RFC 826 ARP (Address Resolution Protocol) resuelve numeros IP a MAC addressses.

RFC 894 especifica cómo se encapsulan los datagramas para transmitirlos por las redes Ethernet.

Internet Layer

Esta es la capa arriba de la Network Access Layer. El "Internet Protocol"(IP) es el corazón de TCP/IP y el protocolo más importante de esta layer. Todos los protocolos en capas superiores e inferiores lo usan para "el delivery" de datos. IP está complementado por ICMP (Internet Control Message Protocol).

IP (Internet Protocol)

IP es el protocolo sobre el que se basa Internet. IP es un protocolo connectionless. (Ver nota). Además se basa en protocolos de otras layers para realizar "error detection y recovery".
Sus funciones incluyen: definición de "datagrama" (la unidad básica de transmisión en Internet), definición del esquema de addressing (números IP y cómo funcionan); definir como mover datos entre la Network Accesss Layer y la Transport Layer, cómo se rutean "datagramas" a hosts remotos, cómo realizo fragmentacion y re-armado de "datagramas".
La figura 6 nos muestra un esquema del datagrama IP.

Versión IP (4 bits)	Longitud de la cabecera (4 bits)	Tipo de servicio (8 bits)	Longitud total (16 bits)			
Identificación (ID) del fragmento (16 bits)			R	DF	MF	Posición de fragmento (13 bits)
Tiempo de vida (TTL) (8 bits)	Protocolo (8 bits)		Suma de comprobación de la cabecera (16 bits)			
Dirección IP de origen (32 bits)						
Dirección IP de destino (32 bits)						
Opciones (longitud variable que se completa con ceros hasta 40 bits)						
Datos						

Figura 6

Recomendamos estudiar este esquema. En otro artículo de esta colección veremos el detalle de cómo se utiliza toda la información en el header.

ICMP (Internet Control Message Protocol). Protocolo de Control de Mensajes de Internet

Es complementario al Internet Protocol y fue definido por el RFC 792. Forma parte de la Internet Layer. Manda mensajes realizando tareas de control como reporte de errores e información de funcionamiento de TCP/IP.

Algunos ejemplos de sus funcionalidades:

Control de flujo: Si los datagramas llegan muy rápido para ser procesados, el host que los recibe o un gateway (router) en el camino, manda el llamado ICMP "Source Quench Masaje" a quien envió el mensaje. Este detiene temporariamente los envíos.

Destinos no accesibles:(Unreachable). Si un sistema se da cuenta que el destino de un paquete es no accesible envía a la fuente (source) un "Destination Unreachable Message". Si el destino no accesible es un host o network, el mensaje lo envía un gateway (router) intermedio. Pero si el destino es un "puerto" no accesible, el host destino envía el mensaje.

Redireccionamiento de ruta: Si un gateway (router) se da cuenta que otro gateway es una mejor opción, le envía al host fuente un "ICMP Redirect Message".

Chequeo de hosts remotos. Un host puede querer saber si otro host está operando. Envía un ICMP "Echo Message". Cuando el segundo host recibe el echo message, contesta reenviando el mismo paquete. El comando "ping" usa este mensaje.
La tabla 1 muestra los códigos que son

utilizados por ICMP para los ejemplos anteriores y otros casos.

Tabla 1

Tipo de código	Mensaje ICMP
0	Respuesta a eco (respuesta a PING)
3	Destino inaccesible
4	Source query
5	Redirección
8	Eco (petición de PING)
11	Tiempo de vida excedido (TTL)
12	Problema en algún parámetro
13	Petición de marca de tiempo
14	Respuesta de marca de tiempo
17	Petición de máscara de red
18	Respuesta de máscara de red

Transport Layer

Los dos protocolos más importantes en esta capa son TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol). TCP nos provee un servicio de entrega de datos confiable. Incluye detección y corrección de errores end-to-end (de punta a punta). UDP provee un servicio de entrega "connectionless" y mucho más reducido. Ambos, además, mueven los datos entre los Application layer y Internet layer dentro de la misma máquina. Quien programe una aplicación dada elegirá qué servicio es el más apropiado.

UDP (User Datagram Protocol)

UDP es un protocolo "connectionless" y no-confiable (no-confiable significando que no existe dentro del protocolo una infraestructura que cerifique que los datos llegan al destino correctamente). El header UDP (ver figura 7) utiliza en la "word1" 16 bits para detallar el Source-Port (puerto fuente) y otros 16 para el Destination-Port (puerto destino). De este modo sabe (por el número de puerto) qué aplicación lo envió y cuál lo recibirá.

¿Por qué decide, quien programa una aplicación, usar UDP?. Puede haber varias razones. Por ejemplo, si la cantidad de datos es muy pequeña, el overhead de crear la conexión y asegurarse la entrega puede ser mayor que re-transmitir los datos. Aplicaciones del tipo pregunta-respuesta son excelentes candidatos. La respuesta misma se puede usar como un aviso positivo de entrega. Si no llega una respuesta en un dado tiempo la aplicación vuelve a enviar su pedido. Puede también ser que una dada aplicación provea su propia infraestructura para entrega confiable y no necesitara una infraestructura más compleja que UDP.

Ver Figura 7

TCP (Transmission Control Protocol) (Procolo de Control de Transmisión)

Las aplicaciones que necesiten que se les provea de una infraestructura confiable usarán TCP. Usando TCP estará segura de que los datos llegaron a destino y en la secuencia adecuada. TCP es un protocolo confiable, "connection-oriented" y "byte-stream".

Un estudio de la Figura 8 y 9 nos indica qué información utiliza para establecer lo que se llama el "three.way hanshake" (estrechado de mano de tres pasos).

¿Por que triunfó TCP/IP sobre otras alternativas?

Son protocolos abiertos, disponibles gratuitamente y desarrollados en forma independiente de cualquier vendor de hardware o sistema operativo.
Son independientes de cualquier hardware físico particular. TCP/IP puede correr sobre Ethernet, Token Ring, línea telefónica dial-up, X.25 net y virtualmente cualquier otro tipo de medio físico de transmisión.
Un esquema de "addressing" (direccionamiento) universal que permite a cualquier dispositivo TCP/IP dirigirse en forma única a cualquier otro dispositivo de la red aún cuando la red sea tan grande como el world-wide Internet.

Figura 7

Número de puerto de origen (16 bits)	Número de puerto de destino (16 bits)
Longitud (16 bits)	Suma de comprobación (16 bits)
Datos	

Protocolos Connection oriented y Protocolos connectionless (no orientado a conección)

Protocolo connection oriented: intercambia información de control con el sistema remoto (llamado handshake - dado de mano), para verificar que está listo para recibir datos antes de enviarlos. Se establece una "connection" en-to-end.
(Ejemplos TCP)
Protocolo connectionless: NO intercambia información de control.

En el word1 (al igual que en UDP) se envía la información de los puertos origen y destino. Pero en este caso es enviada mucha más información.

Application Layer

Protocolos de capa de aplicación

En la capa superior de la arquitectura TCP/IP está la Application Layer. Esta incluye todos los procesos que utilizan a la Transport Layer como medio de entrega de datos.

Es la parte de TCP/IP donde se procesan los pedidos de "datos" o servicios. Las aplicaciones de esta capa estan también esperando pedidos para procesar y están "escuchando" por sus puertos respectivos.

La Application Layer NO es donde está corriendo un procesador de palabras (por ejemplo WORD), una hoja de cálculo o un browser de internet (Netscape o Internet Explorer).

Protocolos

Cuando las computadoras se comunican, es necesario definir un conjunto de reglas que gobiernen su comunicación. Este conjunto de reglas se llaman protocolos.
Los protocolos TCP/IP están disponibles para cualquiera, desarrollados y cambiados por consenso. Y han sido adoptados universalmente, lo que permite la conectividad de redes heterogéneas.



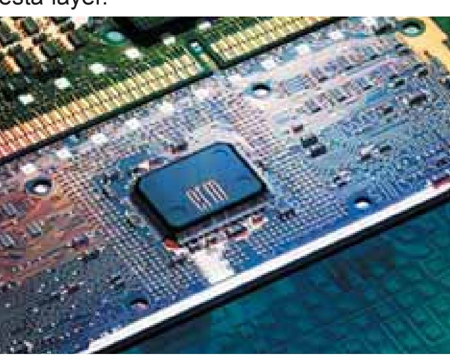
Número de puerto de origen (16 bits)								Número de puerto de destino (16 bits)
Número de secuencia (32 bits)								
Número de acuse de recibo (32 bits)								
Desplazamiento (4 bits)	Reservado (6 bits)	U	A	P	R	S	F	Ventana (16 bits)
Suma de comprobación (16 bits)								Puntero urgente (16 bits)
Opciones (Longitud variable y relleno con ceros)								
Datos								

Combinación de indicadores	**Significado**
SYN	Primer paquete de la conexión que especifica el pedido de comunicación con el equipo destino.
SYN/ACK	El segundo equipo responde y envía su SYN.
ACK	En cada envío se activa este bit para asegurar que el envío anterior se ha recibido correctamente.
FIN	Señal enviada por el equipo que está preparado para cerrar la conexión.
FIN/ACK	Señal enviada por el segundo equipo para aceptar el cierre de conexión y validar el estado de recepción de paquetes.
RST	El paquete RST se envía para dar aviso de recepción de paquetes no esperados. Un caso claro es el de un paquete SYN/ACK que llega sin haber recibido previamente un paquete SYN.

Figuras 8 y 9

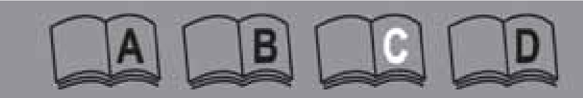
Las aplicaciones que corren en esta capa, SI interactuan con los procesadores de texto, programas de hojas de cáculo y otras.

Los protocolos SMTP, http, Telnet, POP, DNS o FTP son ejemplos de protocolos de esta layer.



Request For Comment (RFC)

La naturaleza abierta de los protocolos TCP/IP requiere documentación pública de los estándares. La mayor parte de la información de TCP/IP se publica como Request for Comments (RFC). Como implica el nombre, el estilo y contenido de estos documentos es poco rígido. Los RFC contienen información bastante completa y no se remiten solamente a las especificaciones formales.



Elementos Básicos de Criptografía

En este artículo expondremos:
- ¿Qué es criptografía?
- Concepto de hash
- Encriptación simétrica: una sola llave
- Encriptación asimétrica: llave-pública y llave-privada
- Entendiendo un algoritmo: el algoritmo RSA

¿Qué es criptografía?

La criptografía es la ciencia que nos permite proteger nuestros datos utilizando una transformación matemática de modo de transformarlos en ilegibles. Algunos ejemplos de su utilización son:

- Cuando necesito enviar / recibir información de un modo seguro a través de una red (intranet, extranet ó internet) la "encriptación" (cifrado) es la herramienta fundamental para poder realizar la tarea.

- Si mi computadora es extraviada y quiero proteger la información almacenada allí.

¿Qué funciones de seguridad me permite realizar la encriptación?

Autenticación: permite a quien recibe un mensaje, estar seguro que quien lo envía es quien dice ser.
Confidencialidad: asegura que nadie leyó el mensaje desde que partió. Sólo el destinatario podrá leerlo.
Integridad: asegura que el mensaje no ha sido modificado.

Para entender como lograr esto detallaremos tres conceptos básicos de criptografía:

A- Algoritmos hash en un sentido
B- Encriptación con llaves (keys, claves) simétricas: se utiliza una llave
C- Encriptación con llaves públicas y privadas: se utilizan dos llaves

En artículos posteriores desarrollaremos infraestructuras que se construyen sobre éstos. Ejemplos: cómo firmar digitalmente un documento o cómo haríamos para intercambiar una llave secreta. El concepto que sigue entender es la llamada Public Key Infrastructure (Infraestructura de llave pública) (PKI) que nos detalla las directivas, los estándares y el software que regulan o manipulan los certificados, y las llaves públicas y privadas. En la práctica, PKI hace referencia a un sistema de certificados digitales, entidades emisoras de certificados (CA) y otras entidades de registro que comprueban y autentican la validez de cada parte implicada en una transacción electrónica.

Hash

Un hash, también denominado valor hash o síntesis del mensaje, es un tipo de transformación de datos. Un hash es la conversión de determinados datos de cualquier tamaño, en un número de longitud fija no reversible, mediante la aplicación a los datos de una función matemática unidireccional denominada algoritmo hash. La longitud del valor hash resultante puede ser tan grande que las posibilidades de encontrar dos datos determinados que tengan el mismo valor hash son mínimas. Supongamos que quiero "hashear" el siguiente mensaje: "mi mamá". Quiero que el mensaje se resuma en un solo número (valor hash). Podría por ejemplo, asociar a cada carácter ASCII su número (ASCII code number) asociado

"m i <espacio> m a m a"

109 + 105 + 32 + 109 + 97 + 109 + 97 = 658.

Así el mensaje se "resumió" (digest) en un solo número. Notemos que ésta es una función en una dirección (no reversible). No hay manera de que alguien adivine el mensaje "mi mamá" a partir del 658 a menos que pruebe todos los posibles mensajes (infinitos) (y calcule su "valor hash (digest)". Aún así tendría muchísimos con 658 y debería adivinar cuál es el correcto (imposible). Destacamos que la función (algoritmo) hash usada fue de lo más simple. En la vida real son usados algoritmos mucho más complejos. Podriamos por ejemplo, usar ese número para verificar si un mensaje enviado fue modificado en el camino: el remitente genera con un algoritmo un valor hash del mensaje, lo encripta y envía el hash encriptado junto con el mensaje. A continuación, el destinatario desencripta el hash, produce otro hash a partir del mensaje recibido y compara los dos hashes. Si son iguales, es muy probable que el mensaje se transmitiera intacto. Aquí supusimos que ambos conocen la llave para encriptar/desencriptar.

Funciones comunes de hash en un sentido

Las dos funciones hash siguientes son las más comunes:

MD5. MD5 es un algoritmo hash diseñado por Ron Rivest que produce un valor hash de 128 bits. El diseño de MD5 está optimizado para los procesadores Intel. Los elementos del algoritmo se han visto comprometidos, lo que explica su menor uso.
SHA-1. Al igual que el algoritmo de llaves públicas DSA, Secure Hash Algorithm-1 (SHA-1) fue diseñado por la NSA e incorporado por el NSIT en un FIPS para datos de hash. Produce un valor hash de 160 bits. SHA-1 es un conocido algoritmo hash de un sentido utilizado para crear firmas digitales.

Encriptación con llaves simétricas: una sola llave

La encriptación con llaves simétricas, es también denominada encriptación con llaves compartidas (shared keys) o criptografía de llave secreta (secret key). Se utiliza una única llave que poseen tanto el remitente como el destinatario. La única llave que es usada tanto para encriptar como desencriptar se llama llave secreta (pero es también conocida como llave simétrica o llave de sesión). La encriptación con llaves simétricas es un método eficiente para el cifrado de grandes cantidades de datos.
Existen muchos algoritmos para la encriptación con llaves simétricas, pero todos tienen el mismo objetivo: la transformación reversible de texto sin formato (datos sin encriptar, también denominado texto no encriptado) en texto encriptado. El texto encriptado con una llave secreta es ininteligible para quien no tenga la llave para descifrarlo. Como la criptografía de claves simétricas utiliza la misma llave tanto para la encriptación como para desencriptar, la seguridad de este proceso depende de la posibilidad de que una persona no autorizada consiga la clave simétrica. Quienes deseen comunicarse mediante criptografía de claves simétricas deben encontrar algún mecanismo para intercambiar de forma segura la clave antes de intercambiar datos encriptados.
El criterio principal para valorar la calidad de un algoritmo simétrico es el tamaño de su llave. Cuanto mayor sea el tamaño de la llave, habrá que probar más combinaciones de diferentes llaves para encontrar la correcta que desencripte los datos. Cuantas más claves sean necesarias, más difícil será romper el algoritmo. Con un buen algoritmo criptográfico y un tamaño adecuado de clave, es imposible, desde un punto de vista informático, que alguien invierta el proceso de transformación y obtenga el texto sin formato del texto encriptado en una cantidad de tiempo razonable.

Algoritmos de claves simétricas:

DES (Data Encryption Standard): El DES nació como consecuencia del criptosis-

tema Lucifer, creado por IBM. Este algoritmo cifra bloques de 64 bits mediante permutación y sustitución. Fue usado por el gobierno de los Estados Unidos hasta que se determinó que no era seguro.

3DES (Triple-DES): La evolución del DES. Utilizando el Standard ANSI X9.52, este algoritmo encripta 3 veces la información y sigue siendo compatible con DES.

AES (Advanced Encryption Standard): Hubo un concurso abierto para analizar qué algoritmo iba a reemplazar al DES. El 2 de octubre de 2000, el NIST anunció el algoritmo ganador: Rijndael, propuesto por los belgas Vincent Rijmen y Joan Daemen (de ahí su nombre). Rijndael es un cifrador de bloque que opera con bloques y claves de longitudes variables, que pueden ser especificadas independientemente a 128, 192 ó 256 bits.

IDEA (International Data Encryption Algorithm): Sistema criptográfico simétrico, creado en 1990 por Lai y Massey, que trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits. Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos, por lo que se ha difundido ámpliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP.

Encriptación con llaves pública: dos llaves (una pública y otra privada)

En la encriptación de llave pública (public key encription) se utilizan dos llaves: una pública y una privada, que se encuentran relacionadas matemáticamente. Para diferenciarlo del cifrado de claves simétricas, en ocasiones el cifrado de claves públicas también se denomina encriptación con llaves asimétricas. En la encriptación de llaves públicas, la llave pública puede intercambiarse libremente entre las partes o publicarse en un repositorio público. Sin embargo, la llave privada será privada a quien cree el par (público/privado). Los datos encriptados con la llave pública sólo pueden descifrarse con la llave privada. Los datos cifrados con la llave privada sólo pueden descifrarse con la llave pública.

Al igual que la criptografía de llaves simétricas, la criptografía de llave pública también tiene diversos tipos de algoritmos. Sin embargo, el diseño de los algoritmos de llave simétrica y de llave pública es diferente. Puede sustituir un algoritmo simétrico por otro simétrico dentro de un programa sin cambios o con cambios mínimos, ya que ambos algoritmos funcionan de la misma manera. Por otro lado, los algoritmos de llave pública que no son iguales funcionan de manera muy diferente y, por tanto, no se pueden intercambiar.

Los algoritmos de llave pública son ecuaciones matemáticas complejas en las que se utilizan números muy grandes. Su principal inconveniente es que proporcionan formas relativamente lentas de criptografía. En la práctica, se utilizan generalmente sólo en situaciones críticas, como en el intercambio de una llave simétrica entre entidades o para la firma de un hash de un mensaje. El uso de otras formas de criptografía, como la criptografía de llaves simétricas, junto con la criptografía de llaves públicas optimiza el rendimiento. También puede combinar la encriptación con llaves públicas con algoritmos hash para producir una firma digital.

Algoritmos típicos de claves públicas

Los tres algoritmos siguientes de llaves públicas son los que se utilizan con más frecuencia:

RSA: para las firmas digitales y los intercambios de llaves. Hoy en día, los algoritmos criptográficos Rivest-Shamir-Adleman (RSA) son los algoritmos de llave pública más utilizados, especialmente para los datos que se envían a través de Internet. El algoritmo toma su nombre de sus tres inventores: Ron Rivest, Adi Shamir y Leonard Adleman. La seguridad del algoritmo RSA se basa en la dificultad (en términos de velocidad y tiempo de procesamiento) de factorización de números grandes. El algoritmo RSA es único entre los algoritmos de llaves públicas utilizados habitualmente ya que puede realizar operaciones tanto de firma digital como de intercambio de llaves. Los algoritmos criptográficos RSA son compatibles con Microsoft Base Cryptographic Service Provider (Microsoft Base CSP1) y con Microsoft Enhanced Cryptographic Service Provider (Microsoft Enhanced CSP2), y están integrados en numerosos productos software, incluido Microsoft Internet Explorer.

DSA: únicamente para firmas digitales. El National Institute of Standards and Technology (NIST, Instituto Nacional de Estándares y Tecnología) de Estados Unidos incorporó el Algoritmo de firma digital (DSA), inventado por la National Security Agency (NSA, Agencia de Seguridad Nacional), al Federal Information Processing Standard (FIPS, Estándar Federal para el Procesamiento de Información) para firmas digitales. El DSA obtiene su nivel de seguridad de la dificultad para calcular logaritmos discretos. Este algoritmo sólo puede utilizarse para realizar operaciones de firma digital (no para la encriptación de datos). Microsoft CSP es compatible con el algoritmo DSA.

Diffie-Hellman: únicamente para el intercambio de llaves. Diffie-Hellman, el primer algoritmo de llaves públicas, recibió el nombre de sus inventores Whitfield Diffie y Martin Hellman. Diffie-Hellman obtiene su nivel de seguridad de la dificultad para calcular logaritmos discretos en un campo finito. El algoritmo Diffie-Hellman puede utilizarse únicamente para el intercambio de llaves. Microsoft Base DSS3 y Diffie-Hellman CSP son compatibles con el algoritmo Diffie-Hellman.



Explicación matemática del algoritmo RSA

El sistema RSA se basa en la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más común consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número.

Si el número considerado es un número primo (el que sólo es divisible por 1 y por él mismo), para factorizarlo habría que empezar por 1, 2, 3,… hasta llegar a él mismo, ya que por ser primo, ninguno de los números anteriores es divisor suyo. Y si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.

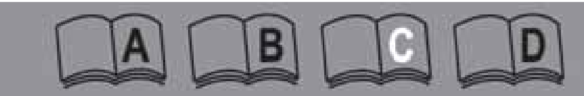
Basado en la exponenciación modular de exponente y módulo fijos, el sistema RSA crea sus claves de la siguiente forma:

1. Se buscan dos números primos lo suficientemente grandes: p y q (de entre 100 y 300 dígitos).
2. Se obtienen los números n = p * q y Ø = (p-1) * (q-1).
3. Se busca un número e (e menor que n) tal que no tenga múltiplos comunes con Ø.
4. Se encuentra d tal que (ed-1) sea divisible por Ø.

Y ya con estos números obtenidos, e es la clave pública y d es la clave privada. Los números p, q y Ø se destruyen. También se hace público el número n, necesario para alimentar el algoritmo. El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo).

RSA basa su seguridad es ser una función computacionelmente segura, ya que si bien realizar la exponenciación modular es fácil, su operación inversa, la extracción de raíces de módulo Ø no es factible a menos que se conozca la factorización de d, clave privada del sistema.



Algoritmos de hash seguros

¿(In) seguros?

Autor: Juan Manuel Zolezzi

Durante la CRYPTO 2004 tres grupos de cripto-analistas probaron que las funciones Hash más utilizadas estarían "rotas". ¿Qué significa? ¿Qué implica? ¿Cómo nos impacta este descubrimiento?

Analisis de las "colisiones" comprobadas recientemente en MD5 y otras funciones hash.

Durante la CRYPTO 2004 tres grupos de cripto-analistas probaron que las funciones Hash más utilizadas estarían "rotas". ¿Qué significa? ¿Qué implica? ¿Cómo nos impacta este descubrimiento?

Uno de los principales "pilares" sobre los que se yergue la criptografía moderna es el de la capacidad de identificar inequívocamente a un mensaje y diferenciarlo de otro tan sólo ligeramente distinto. Es incluso tan importante que todo DSA ("Data Signature Argorithm" - Algoritmo de Firma de Datos) se arma en torno a él, en torno a "la capacidad de obtener de un mensaje arbitrariamente largo, un número de longitud fija", número al cual se convino en denominar: "firma".

Ahora, esta "firma" haría las veces de "huella digital"; la analogía es directa, ya que si fuera éste el ÚNICO método que tuviéramos para diferenciar a una persona de otra (y de establecer que dicha persona es en verdad quien dice ser) nos encontraríamos en igualdad de condiciones con los DSAs. Imagínense ahora que cabiese la posibilidad (mejor aún, que se haya dado el caso) de encontrar a dos personas DISTINTAS con LA MISMA huella digital, TODO lo que se hubiera basado en la correspondencia "uno en uno" de personas a huellas digitales pierde todo sentido, ya que en este caso no nos es posible diferenciarlas.

El Problema:

Es exactamente esto lo que (aunque se sospechaba desde un principio) se dio a conocer definitivamente durante la CRYPTO 2004, la mayor conferencia anual sobre criptografía, en su 24ª edición, cuando tres grupos de investigadores por separado probaron la relativamente alta probabilidad de hallar "colisiones" (el hecho de ser dos firmas iguales SIN pertenecer al mismo dato) en las funciones HASH (los procesos mediante los cuales se generan éstas).

Gran parte del trabajo de un cripto-analista consiste en encontrar, para una función Hash dada, situaciones (si bien teóricas) bajo las cuales sea posible encontrar colisiones. Un número moderado de colisiones bajo condiciones relativamente restrictivas es normal, pero lo que estos grupos hallaron fueron probabilidades inusualmente altas de hallar colisiones en las funciones Hash más utilizadas, de allí la importancia del "problema".

Lo que implica:

Ahora bien, ¿qué significa (para el resto de los mortales) que se hayan encontrado colisiones?
Bueno, como en la mayoría de los casos, el daño al darse cuenta de una falla depende de cuánto se dependa de ella; en este caso particular: MUCHO. El problema es que con el correr de los años y los avances de la criptografía gran parte de las tareas diarias (tanto dentro como fuera del ámbito informático) se han ido tornando "cripto-dependientes". Por ejemplo: cada vez que se ejecuta un programa en Windows XP, el mismo kernel genera un Hash de éste y lo chequea para ver si posee el "logotipo de Windows"; si la función Hash que utilizara estuviera rota, un atacante podría aplicar un troyano a nuestro programa en teoría "legal" y XP no notaría la diferencia ya que ¡AMBAS FIRMAS SERÍAN IGUALES! (1). No vamos a entrar en detalles sobre qué ámbitos se encontrarían comprometidos y cuáles no, pero es bastante seguro que la lista sería MUY larga e implicaría sin ninguna duda una amenaza para la privacidad individual.

Malas noticias:

Cinco de las más usadas funciones de Hashing se encuentran en este momento "comprometidas": SHA0 ("Secure Hash Algorithm Rev.0" - Algoritmo Seguro de Hash Revisión 0), MD5 ("Message Digest 5" - Digestión de Mensajes Versión 5), HAVAL, MD4 (hermano menor de MD5), y RIPEMD; la función sobre la cual se había depositado toda la confianza para llegar a satisfacer los requisitos de seguridad hasta el año 2010, SHA1 (hermano mayor de SHA0), se encuentra ahora "bajo sospecha" y todavía queda por evaluar el estado de su sucesora SHA2.

Las MALAS NOTICIAS vienen de la mano de la ingeniería de software; infinidad de aplicaciones y servicios considerados hasta el momento "infalibles" se ven ahora frente a un futuro incierto al mismo tiempo que la confianza en ellas depositada (que en última instancia es lo único que cuenta en este ámbito) se tambalea peligrosamente. Es probable que estemos viendo los albores de una crisis similar a la Y2K, ya que la cantidad de software a "reparar" es incalculable (como lo son también los gastos que ello significaría).

Para los usuarios la amenaza que esto implica es directa, ya que representa una grieta profunda en todas las herramientas con las que actualmente se cuenta a la hora de proteger la privacidad individual. Esto se hace extensivo a todos los ámbitos, ya que bajo esta premisa no es ya seguro el manejo que se hace de los datos personales (nombres, direcciones, documentos, cuentas bancarias, números de tarjeta de crédito, etc.) por parte de las instituciones, así como tampoco lo es el manejo que hacen éstas de los suyos propios (secretos industriales, balances, información financiera, etc.).

Conclusión en este respecto: de extenderse esta brecha, las consecuencias pueden ser más que importantes, y lo que es más pueden afectar a una porción significativa de los usuarios eventuales.

Buenas noticias:

Si bien el panorama se tornó súbitamente lúgubre para quienes dependemos de estas herramientas, no todo está perdido (para hacer honor a la verdad, aún NADA se ha perdido).

Cabe a esta altura aclarar en mayor detalle el tipo y alcance de los descubrimientos teóricos al respecto. Los descubrimientos se basaron en métodos teóricos de alta complejidad (salvo el método expuesto por el Dr. Dengguo Feng, mediante el cual las colisiones para MD4 podrían calcularse "a mano" con nada más que papel, lápiz y una calculadora científica). Otro aspecto a tener en cuenta es que las colisiones sólo se han probado altamente probables (valga la redundancia) pero un uso práctico de ellas aún queda por verse. Cabe explicar esto último con más detalle: si bien las colisiones existen y se han probado, los textos que generan la misma firma (aquellos "que colisionan") no guardan relación entre sí, de manera tal que no se pueden prever fines prácticos para ellas; existe la posibilidad de que se perpetren actos de "vandalismo informático" en los cuales no se busca ganar el acceso (a través de la "confianza" depositada en la firma en sí), sino tan sólo intercambiar un mensaje con sentido por otro que nada significa pero que comparte la misma firma que el original, perdiéndose éste y obteniendo "basura" como resultado.

Conclusión en este respecto: no hay necesidad de entrar en pánico, si bien el hecho de que estas colisiones siquiera existan representa un punto débil en los esquemas de firma digital, pasará aún mucho tiempo hasta que puedan tornarse un problema mayor. Para los ingenieros en software: es mejor evitar las funciones Hash "dudosas" o "rotas" y se recomienda la migración a funciones de la familia de algoritmos SHA1 o SHA2 (2).

En fin:

¿Representa un peligro? Sí. ¿Habría que preocuparse? También.
¿Representa un peligro INMINENTE? No. ¿Habría que preocuparse MUCHO? Tampoco.

Referencias:

RSA Security: http://www.rsasecurity.com (4)

RSA Laboratories (centro académico de RSA Security): http://www.rsa.com

NIST (EE.UU.) ("National Institute of Standards and Technology" - Instituto Nacional de Estándares y Tecnología): http://www.nist.gov

CRYPTO 2004: http://www.iacr.org/conferences/crypto2004

Homework:

- ¿Qué es un "Hash"? ¿Qué es una "función Hashing"?
Un Hash es el valor retornado por una "función Hashing" o "función Hash".

Una función Hash es una primitiva que se utiliza en varios ámbitos, desde la criptografía hasta las búsquedas en tablas ("Hash-tables" - Tablas "Hasheadas"). Estas funciones toman un texto, dato o mensaje y generan un número (usualmente MUY grande) de longitud fija. Pero una función Hash debe reunir una serie de condiciones para resultar práctica, y éstas se vuelven mucho más restrictivas a la hora de empleárselas en criptografía (se dice entonces que son "cryptographically safe" - criptográficamente seguras). Básicamente deben ser "one-way" (en un solo sentido) y "collision-resistant" (resistentes a colisiones). ¿Qué significa esto?:

One-way ("en un solo sentido"): debe ser relativamente fácil generar el Hash a partir del mensaje, pero debe ser "computacionalmente imposible" generar el mensaje a partir del Hash.

Collision-resistant ("resistentes a colisiones"): la probabilidad de encontrar dos textos que generen el mismo Hash debe ser cuasi nula y los textos que colisionen no deben guardar relación.

- Colisiones: ¿Por qué no se pueden evitar?
Como dijimos antes, una colisión se da cuando dos mensajes distintos generan el mismo Hash.
Como también dijimos anteriormente las colisiones se "sospechaban desde un principio". Esto no es totalmente correcto, ya que desde un primer momento se SABE que existirán colisiones. ¿Por qué? por la misma razón por la que no puede existir un algoritmo de compresión de razón independiente (3):
Consideremos un alfabeto de 26 letras y mensajes de 20; la cantidad de mensajes distintos posibles es 26^20 o 19.928.148.895.209.409.152.340.197.376: MUCHOS.
Supongamos que queremos generar un Hash con el mismo alfabeto, pero de 10 caracteres; la cantidad de Hashes distintos es ahora: 26^10 o 141.167.095.653.376: muchos también, pero MENOS que la cantidad de mensajes.
¿Qué significa esto? simple: que no hay suficientes Hashes para todos los mensajes, por lo tanto SIEMPRE va a haber colisiones.

Una última nota: los mensajes del ejemplo no tenían más de 20 letras, consideren lo que sucede en el mundo real, donde los mensajes tienen varios cientos de MILLONES de caracteres...

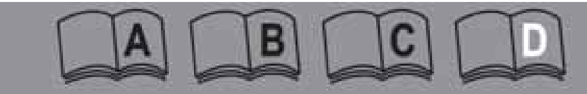
(1) Esto es, en realidad, ligeramente más complicado y se lo denomina "ataque de segunda preimagen" (partir de un archivo original y generar uno distinto que posea su misma firma) aunque estrictamente sería relativamente fácil a partir de los datos obtenidos hasta el momento.

(2) Los laboratorios RSA ("RSA Laboratories") ya habían sugerido la migración a los algoritmos SHA1 en el año 1996.

(3) Un algoritmo de compresión de razón independiente es uno con el cual se puede comprimir un mensaje SIEMPRE a la misma razón (al mismo x%), independientemente del contenido del mensaje. Cabe aclarar que nos referimos a algoritmos de compresión "lossless" (sin pérdidas), ya que un algoritmo "lossy" (con pérdidas), como por ejemplo: Jpeg, la familia MP, DivX, etc.) siempre puede dejar de lado parte del mensaje y llegar a una razón fija de compresión. Este fenómeno fue analizado desde el punto de vista de la transinformancia y la entropía dentro de un mensaje por el genial C. E. Shannon en su tesis "A Mathematical Theory of Communication" (Una Teoría Matemática de la Comunicación) en la cual se basa la teoría de la mayoría de los algoritmos de compresión sin pérdidas de hoy en día (Huffman, Lempel-Ziv, etc.).

(4) RSA Security es la empresa de criptografía de mayor renombre en el mundo, fundada por Ron Rivest uno de los inventores del primer esquema de llaves públicas, mejor conocido como RSA (siglas de los inventores: R. L. Rivest, A. Shamir, L. M. Adleman).





EL GRAN DEBATE: PASS PHRASES vs PASSWORDS

Parte 1 de 3

por Jesper M.Johansson
PhD.,ISSAP,CISSP
Supervisor del Programa de Seguridad.
Corporación Microsoft

La seguridad informática presenta debates interesantes. Los tópicos varían en importancia, pero todos demuestran que el tema es excitante y sigue creciendo. Me gustaría resumir algunos de estos debates, y además ofrecer mi punto de vista personal. En la primera parte de estos artículos, introduciré el tema de passwords y explicaré el debate de pass phrases vs. passwords.

En realidad podría discutirse si "pass phrases vs. passwords" es realmente el gran debate o algo aburrido que no le interesa a mucha gente. De cualquier manera ¿cuál es más seguro? La respuesta no es tan clara como aparenta.
De manera de analizar el tema dividí el artículo en tres partes. En la primera se cubren los temas fundamentales de pass phrases y passwords y se describe como se guardan y otros temas. En la próxima entrega describiré la fortaleza de cada uno y aplicaré algunos argumentos matemáticos con el propósito de determinar cual es más fuerte. En la última entrega arribaré a la conclusión de la serie y ofreceré una guía de cómo elegir un password y configurar una política de password.

Algunos fundamentos

Lo primero y más importante es comprender la diferencia entre pass prhase y password. Cuando la mayoría de la gente selecciona un password elige una palabra como "password" o una serie de símbolos al azar como "X2!aZ@<dF:" o alguna combinación de las dos como "P@s$w0rd". Un pass phrase es una frase, como por ejemplo "Éste es realmente un pass phrase complejo". Un pass phrase es típicamente más largo que un password y contiene espacios. Alguna gente construye un password seleccionando la primera letra de cada palabra de una frase. Ese password no constituye un pass phrase; es un password hecho con una lógica interesante. Un pass phrase en contraste, es diferente de un password basada en símbolos (token-based), donde ahora los tokens son palabras en vez de símbolos escogidos entre un grupo de caracteres. Un pass phrase no necesariamente será una frase correctamente deletreada, libre de sustituciones de símbolos, como los usados en el ejemplo anterior.
Las diferencias claves entre pass phrase y password son:
(1) Un pass phrase usualmente contiene espacios, los passwords no.
(2) Un pass phrase es más largo que la gran mayoría de las palabras, y, lo más importante, es más largo que un grupo de letras elegidas al azar, que cualquier persona pudiera recordar.
A pesar de que un pass phrase puede ser simplemente considerado como un password muy largo, típicamente se constituye de una secuencia de palabras, o algo similar a palabras. En particular, las pass phrases que elegiré en estos artículos son compatibles para el uso con Windows 2000 y más actuales. Otros productos usan pass phrases de acceso con características diferentes, o puede ser que no las acepten.

Como segundo concepto usted necesita entender la diferencia entre password guessing (en inglés, adivinar el password) y password cracking (en inglés, romper el password).El password guessing es cuando alguien se sienta en la consola o en una máquina remota probando passwords. Adivinar no es relevante a este artículo, porque si una cuenta tiene un password relativamente complejo, el adivinarlo no será exitoso de cualquier manera. Si la adivinanza es exitosa puede ser por suerte increíble del atacante o porque el password era débil.

Miremos un ejemplo. Primero considere que los passwords permiten cuatro categorías de símbolos: mayúsculas, minúsculas, números y no-alfanuméricos. Los símbolos no-alfanuméricos incluyen todos los del teclado, así como todo lo que no se muestra en el teclado, como los caracteres Unicode. Algunas personas consideran a los caracteres Unicode y los símbolos del teclado como dos categorías diferentes. Nosotros los pensaremos como dentro de la misma categoría. Aún más, para todos los propósitos el término "carácter" se referirá a las cuatro categorías colectivamente. Por ejemplo, asumamos que los passwords que hemos elegido son palabras no-de-diccionario, que usamos ocho caracteres con por lo menos tres o cuatro tipos diferentes y que expirarán en 70 días. Para que un atacante sin conocimiento previo de ninguno de estos passwords, pudiese adivinar uno de ellos antes de que expire, requeriría que la computadora tuviese un ancho de banda equivalente a 53.000 T-3 (44.736 Mbps cada uno). Esto es lo que se requeriría solamente para mandar el tráfico de autenticación, de modo de poder probar la mitad de todos los passwords posibles (asumiendo que cada uno es igualmente probable).

Si restringimos el conjunto de caracteres para adivinar, a los 76 símbolos más comunes y asumimos que el password es seleccionado al azar, o que así lo ve un atacante, hay 1.11 x 10^5 passwords posibles de 8 caracteres. Si el atacante adivina 300 de éstas por segundo, lo que es muy difícil incluso con los programas más optimizados, le tomaría 58.783 años para adivinar el password. Si el atacante simplemente "scriptea" (hace uso de un script) el comando "net use", podría como mucho hacer dos o tres intentos por segundo, lo que significa que le tomaría 5.878.324 años adivinar el password.

Cracking, por otro lado, se puede realizar después que el atacante ha obtenido los "hashes crudos" (raw hashes, es decir los hashes puros). (Un hash es una representación matemática usualmente utilizada para guardar passwords. Nosotros lo discutiremos en mayor detalle más abajo) El atacante genera passwords de prueba, los hashea y entonces los compara con los hashes almacenados. Cracking es mucho más veloz que adivinar (guessing). Incluso usando hardware moderado, un atacante puede generar y probar 3.000.000 de passwords por segundo. Un ataque de cracking contra todos los passwords generados con 8 caracteres y utilizando un conjunto de 76 caracters posibles, basándonos en la cifra anterior, llevaría no menos de 6 años. Por

supuesto muchos de los passwords serían encontrados en menor tiempo, y para cualquier password dado será estadísticamente encontrado en la mitad de ese tiempo. Si los passwords son sólo de 7 caracteres, crackear todos los passwords tomará solo 28 días aproximadamente.
Cómo el atacante obtiene los hashes, es un tópico abierto, así como si el cracking es una preocupación primaria. Considere que en Windows el atacante necesita tener un nivel de acceso de "system, o ADMINISTRATOR" a un domain controler (DC, controlador de Dominio en Active Directory) para poder crackear el password de dominio. Si un atacante ya ha comprometido un domain controler, crackear las passwords es sólo un problema secundario. Sin embargo, la mayoría de los atacantes realizan el cracking de los passwords. ¿Por qué? Mayormente, porque el atacante espera que alguno tenga una cuenta en un sistema diferente, en otro dominio con el mismo nombre de usuario y password. Eso es conocido como una "dependencia administrativa", un tópico que trataremos en un artículo futuro. Aún más, como el único secreto usado en un protocolo de tipo challenge-response (desafío-respuesta) es el hash del password, crackear el password es de algún modo superfluo porque los hashes son todo lo que el atacante necesita para acceder a la cuenta. De cualquier manera, los atacantes típicamente crackean los passwords y su posibilidad de éxito es alta siendo esto un serio problema.

Tenga presente que los sistemas operativos modernos no guardan usualmente passwords o pass phrases en texto plano. Normalmente, el valor guardado es el resultado de una función one-way (de sentido único), como el hash. En los sistemas operativos basados en Windows NT (incluyendo Windows 2000, XP y Server 2003) el password está guardado de diferentes maneras. Las representaciones más comunes son el hash-LM (Lan Manager) y el hash-NT. Para los propósitos de este artículo usted no necesita saber exactamente cómo trabajan. Solamente necesita saber tres cosas:

El hash LM es "case-insensitive" (no sensible a mayúscula- minúscula), mientras el NT hash es "case-sensitive" (sensible a mayúscula- minúscula).

El hash LM tiene un set de caracteres limitado a sólo 142, mientras que el has NT soporta casi enteramente el conjunto de caracteres de Unicode de 65.536 caracteres.

El hash NT calcula el hash basándose en el password entero que el usuario ingresó. El hash LM corta el password en dos trozos de 7 caracteres cada uno, haciendo padding (acolchonado, acción de completar) si es necesario.
Ambos tipos de hashes generan un valor de 128 bits que es guardado. La mayoría de los crackers de password, hoy crackean el hash LM primero y luego crackean el hash NT simplemente probando todas las combinaciones mayúscula minúscula del passwords "case -insensitive" obtenido del hash LM.

El hash LM es una función one-way muy débil usada para guardar passwords. Originalmente inventada para el sistema oiperativo Lan Manager, el hash LM fue incluido en Windows NT para tener compatibilidad con sistemas legacy (anteriores). Todavía se encuentra incluido por compatibilidad con anteriores sistemas operativos. Debido a la forma en que el password hash LM es calculado, ningún password con un hash LM es más fuerte que un password de 7 caracteres elegido de un conjunto de 142 caracteres.

Removiendo los hashes LM

Existen muchas maneras de asegurarse que el Hash LM no sea guardado. Una de ellas es usar passwords o pass phrases más largas de 14 caracteres. Se puede también usar el switch NoLMHash que aparece en la Política de Grupo (Group Policy) de Windows Server2003 y Windows XP como "Network security: no guarde el valor del hash Lan Manager en el próximo cambio de password". Usando ese switch globalmente desactiva el guardado de los hashes LM para todas las cuentas. El cambio se va a llevar a cabo la próxima vez que el password se cambie. Los hashes LM ya existentes para el password actual y cualquier password pasado no son removidos con simplemente activar ese switch. Es más, el hecho de que los efectos de ese switch no sean inmediatos significa que no notará enseguida cualquier problema potencial causado por no guardar los hashes LM. Vea el artículo de Conocimientos Básicos de Microsoft (Knowledge Base), KB 299656 para mayor información. El artículo del KB también tiene información sobre cómo usar el switch NoLMHash con Windows 2000.

Usted puede también remover el hash LM utilizando ciertos caracteres en su password. Es ampliamente creído que usando caracteres ALT en su password se previene que los hash LM sean generados. En realidad, sólo algunos de los caracteres Unicode provocan que los hashes LM desaparezcan. Por ejemplo los caracteres Unicode entre 0128 y 0159 provocan que el hash LM no sea generado. Algunos caracteres Unicode son convertidos en otros caracteres antes de ser hasheados.
Existe una preocupación con la remoción de los hashes LM. ¡Hacerlo hará que ciertas cosas dejen de funcionar! Una razón por la cual los hashes LM son dejados activos por default es porque removiéndolos genera problemas sobre cualquier aplicación que use autenticación basada en UDP para RPC (Remote Procedure Call). Esto incluye los Servicios de Cluster de Windows, el Servidor de Comunicación de Tiempo Real, y probablemente otros. Estos problemas se solucionan activando el seteo NtlmMinClientSec, que aparece expuesto como "Network Security: Seguridad mínima de la sesión para clientes basados en NTLM SSP (incluyendo secure RPC)" en Políticas de Grupo en Windows Server 2003. NTLMinClientSec necesita ser seteado como mínimo a "Requiere integridad de mensaje" y "Requiere NTLMv2 Session security (0x80010)". Cuando se setea de ese modo RPC utiliza autenticación NTLMv2, que usa el hash NT(Vea el artículo KB828861 para más información en problemas de cluster cuando usted no tiene un hash LM). Otras aplicaciones también dejan de funcionar en ausencia de un hash LM. Por ejemplo el Outlook 2001 para la Macintosh requiere que todas las cuentas que usará tengan uno. Windows3.x definitivamente tiene problemas sin un hash LM, y Windows 95 y 98 en algunos escenarios. Además algunos productos de terceros, como los dispositivos de almacenamiento adjuntos a la red, pueden requerir hashes LM.

Comentarios finales:

Esta primera entrega de la serie de artículos sobre passwords ha tratado sobre lo básico de los passwords. En la próxima trataremos de analizar si las pass phrases tienen una ventaja real sobre los passwords. De cualquier manera, dado la poca cantidad de gente que los usa actualmente, tenemos muy pocos datos reales de las pass phrases. De manera de entender más de ellas, deseamos pedirle un favor. Si usted desea ayudarnos, piense en una pass phrase que usted podría usar (de preferencia no la que usted usa actualmente) y envíela por mail a passstud@microsoft.com. Esperamos recibir suficientes resultados de manera de hacer algún análisis de pass phrases y comprender cómo están estructuradas en la realidad. Como siempre, esta columna es para usted. Déjenos saber si hay algo que usted desee discutir, o si hay una mejor manera en que lo podamos ayudar a asegurar su sistema.

Este artículo también apareció en “Microsoft Security Newsletter, Vol 1 Issue 13” (gratuito) al que recomendamos suscribirse.



Introducción

ETHICAL HACKING PASO A PASO

"Si conoce al enemigo y se conoce a sí mismo, no debe temer por el resultado de cientos de batallas. Si se conoce a sí mismo, pero NO al enemigo, por cada victoria obtenida sufrirá una derrota. Si no conoce al enemigo ni a sí mismo, sucumbirá en todas las batallas"

"El arte de la guerra", Sun Tzu

Paso 0. Introducción

Ethical Hacking Paso a Paso estará compuesto por una serie de artículos, básicamente sobre "metodologías y las herramientas" de hacking y las contramedidas (countermeasures). Para cada acción de hacking existen diversas herramientas. Algunas de ellas son puntuales para una acción y otras abarcan un abanico de ellas, lo que las hace muy completas y poderosas. Nosotros detallaremos aquellas más populares y/o que consideremos excelentes para ejemplificar una dada acción. En la sección TOOLS (herramientas) encontrará detalle de las herramientas más destacadas del mundo de la seguridad informática.

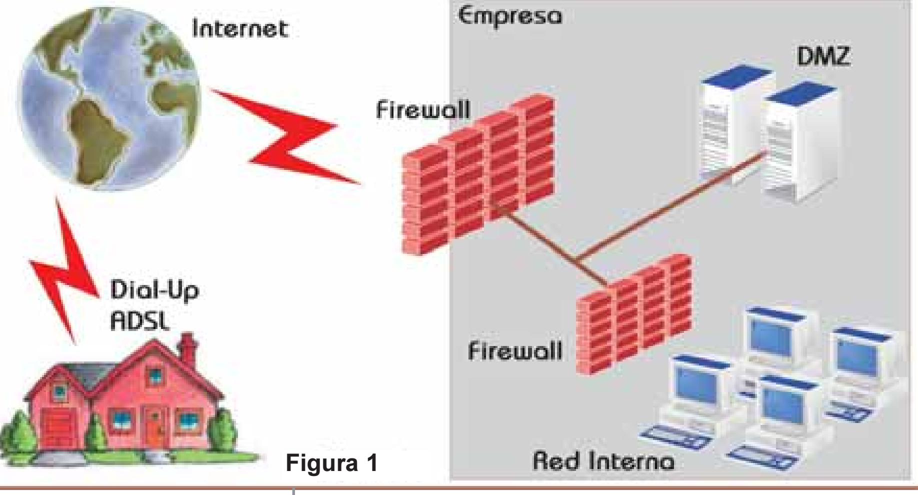


Figura 1

Las personas interactuando con los dispositivos, conforman una comunidad. Dentro de esa comunidad existen buenos y malos.

Entendiendo al enemigo

"Si conoce al enemigo y se conoce a sí mismo, no debe temer por el resultado de cientos de batallas. Si se conoce a sí mismo, pero NO al enemigo, por cada victoria obtenida sufrirá una derrota. Si no conoce al enemigo ni a sí mismo, sucumbirá en todas las batallas"

"El arte de la guerra", Sun Tzu.

Conocer a nuestro enemigo es tan complejo como conocerse uno mismo. A veces los administradores conocen a su enemigo sólo a través de "su idea" sobre él. Muchas veces esa idea nada tiene que ver con la realidad. Por ejemplo, en algunas películas se muestra a alguien accediendo a los recursos de una computadora mediante la rotura de una llave de encriptación. Se muestra al atacante tipeando la clave, adivinándola y lo resuelve en segundos. O escribe un programa con una interfase gráfica con grandes número donde puede crackear cada carácter de la clave uno por uno. Estas simulaciones son totalmente irreales y nada tienen que ver con los conceptos matemáticos que gobiernan las metodologías de encriptación.

Entendiendo el problema



Describamos el esquema de la Figura 1. Nos muestra una empresa con dos firewalls back-to-back y una DMZ (Demilitarized Zone-Zona Desmilitarizada, donde ubicamos, por ejemplo, nuestros web-server, DNS, ftp-server, etc. Es decir servidores expuestos al mundo), un hogar y una nube (Internet).

Pero ¿qué representa esa nube?. Si incluyésemos en ese esquema a más hogares y a más empresas, a miles o millones de ellas obtenemos lo que se llama Internet, o sea la nube.

Los elementos que componen la llamada red-de-redes (Internet), son dispositivos (hardware: CPUs, hubs, switches, firewalls, routers y otros), conexiones (por ejemplo: cables UTP, antenas para wireless, fibra óptica), programas (sistemas operativos como Linux, Windows, Unix, NetWare y aplicaciones como Office, Dreamweaver, The Gimp) y personas.

Las personas interactuando con los dispositivos, conforman una comunidad. Dentro de esa comunidad existen buenos y malos.

El término "hacker" nació



asociado a los entusiastas de la computación interesados en aprender sobre los lenguajes de computación y los sistemas de cómputo.

Estudiando los programas, detectando los errores de programación (bugs o flaws) e individualizando aquellos que permiten obtener privilegios a partes del sistema a los cuales no se está autorizado, detectan las "vulnerabilidades". Y, tan pronto un hacker descubre o alguien anuncia una vulnerabilidad, aparece el "exploit" (herramienta que se aprovecha de esa vulnerabilidad). Hoy el término se refiere a individuos que ganan acceso no-autorizado a sistemas de cómputo con el propósito de robar o corromper información. Los hackers mantienen que el nombre apropiado sería "cracker".

Así, hoy se dice: hackeo un sistema (una computadora), hackeo una red (aprovecho un firewall mal configurado), hackeo un web-server (aprovecho una vulnerabilidad de Apache o el IIS).

El propósito de algunos hackers es decir: "lo hice". Dejan una marca o evidencia mostrando su habilidad. Para otros el fin es dañar: cometer algún delito fraudulento o simplemente destruir.

El hacking solía ser tarea de unos pocos expertos muy capacitados. Hoy, existen un sin número de herramientas pre-hechas con las que solo hace falta apuntar a nuestro "target" (objetivo) y hacer clic. Son herramientas de destrucción muy poderosas capaces de causar mucho daño a nuestra "cyber-comunidad".

¿Cómo hacemos entonces para protegernos de los Hackers?

La respuesta es conocer. Para poder mejorar la seguridad y protegernos debemos conocer bien las modalidades usadas por los hackers. Los hackers cuentan con innumerables herramientas y metodologías que no podemos desconocer. Ellos, debido a su naturaleza se reinventan continuamente al igual que a sus técnicas.

El profesional de seguridad deberá por tanto conocer muy profundamente el ámbito de ataque y la filosofía de los atacantes de modo de poder ayudar a las empresas respecto de su seguridad.

Deberá crear medidas concretas haciendo la infraestructura IT de las empresas menos vulnerables.

En los últimos años ha aparecido el concepto de "ethical hacker". Este, es alguien, quien dotado de las mismas herramientas que el hacker las utiliza para testear (penetration testing- test de penetración) nuestra red. Su expertise es tal que realizando tal test puede darnos el panorama de cuáales son nuestras debilidades al poner nuestra empresa conectada en una intranet o a Internet.

Nota: es muy importante saber que 50% de los eventos de seguridad provienen de nuestras redes internas.

En esta tarea de "conocer" han aparecido un gran número de libros, conferencias, eventos divulgando las técnicas de hacking buscando de mostrar cómo opera el enemigo.

En cada artículo expuesto en NEX IT Specialist, daremos bibliografía, pero aquí queremos destacar la serie de libros cuyos autores pertenecen a una de las empresas más prestigiosas de Seguridad Informática (Foundstone Inc.: www.foundstone.com): www.hacking-exposed.com. Casi todos han sido traducidos al español y editados en McGraw Hill/InterAmericana de España (lamentablemente las traducciones son paupérrimas!!!. Excepto el de "Hackers en Linux").

Instituciones privadas y gubernamentales también le han dado marco a toda una serie de actividades educativas y de divulgación. Destacamos el SANS Institute (www.sans.org), el ICS2 (www.ics2.com) creadora de la prestigiosa certificación CISSP. The International Council of Electronic Commerce Consultants (EC-Council®) (http://www.eccouncil.org), The Institute for Security and Open Methodologies (ISECOM) www.isecom.org donde se definen estándares en tests de seguridad y testeo de la integridad de los negocios.

Paso 1: Footprinting

Recolección de información

Autor: Juan Manuel Zolezzi

La importancia del footprinting

Una de las acciones más importantes a la hora de hackear un sistema (o intentar) es obtener la máxima información disponible sobre él. En definitiva se trata de obtener las versiones de sus sistemas operativos, los puertos que tiene abiertos y toda información que nos pueda ser útil.

Visual Route proporciona información de las rutas y también la localización geográfica. .
http://www.visualroute.com

Cuando un ladrón se dirige a un Banco con intenciones de robarlo, él no sólo camina al mostrador y dice "arriba las manos". Primero se toma su tiempo para recolectar la información necesaria para que su obra sea perfecta. Información sobre rutas de los autos blindados, los tiempos de entrega, cámaras de video, salidas de escape y un sinfín de detalles que lo ayudarán a cometer el delito con éxito.

Lo mismo sucede con los hackers cuando se plantean hackear un sistema, primero comienzan con lo que se llama "systematic footprinting", que simplemente es obtener información relevante como para crear un perfil de la configuración de seguridad de dicho sistema, organización, etc.

Cómo realizar el footprinting

Resulta difícil dar una guía de cómo efectuar el footprinting (a veces llamado "actividades de rastreo"), ya que es una actividad que puede conducir a varios caminos posibles. Sin embargo, aquí esbozamos algunas acciones que muestran como se realiza dicho análisis.

Determinar el alcance del análisis

El primer punto a resolver es determinar el ámbito de las actividades de rastreo. ¿Se va a analizar la estructura de toda una empresa o bien limitar a ciertas ubicaciones (por ejemplo, sedes o filiales)? En ciertos casos, la tarea de determinar todas las entidades asociadas a una empresa puede ser un tanto complejo. Internet pone a nuestra disposición del hacker una gran cantidad de recursos que podrá utilizar y que le ayudarán a reducir el ámbito de sus actividades, así como también ideas sobre el tipo y cantidad de información pública de una empresa y sus empleados.

Como punto de partida el hacker examinará la página web de la empresa objetivo, si es que tiene una. Muchas veces una página web de una empresa proporciona una cantidad increíble de información que puede ayudar a los atacantes. Se ha llegado a ver incluso las opciones de configuración de seguridad de sus firewall en los servidores web de Internet de algunas empresas. Otros puntos de interés son:

>>Ubicaciones

>>Compañías o entidades relacionadas

>>Noticias de fusiones o adquisiciones

>>Números de teléfono

>>Nombres de contacto y direcciones de correo electrónico

>>Directivas de seguridad o privacidad que indiquen los tipos de mecanismos de seguridad instalados

>>Enlaces a otros servidores web relacionados con la empresa

Ahora lo que hará es identificar nombres de dominio y redes asociadas relacionadas con la empresa en particular. Los nombres de dominio representan la presencia de la compañía en Internet y son, en Internet, el equivalente al nombre de su compañía, por ejemplo, "nombre-empresa.com.ar".

Existen numerosas bases de datos que podrá consultar y que proporcionan gran cantidad de información sobre las distintas entidades cuyo rastro esté intentando seguir. Hasta hace un tiempo, la compañía Network Solutions tuvo el monopolio como registro principal de los nombres de dominio: .com, .net, .edu y.org), pero en la actualidad existen numerosos registros disponibles.

Si dispone de un sistema operativo tipo UNIX, podrá utilizar el comando "whois" o "xwhois". En Windows, utilizará programas como "Netscan" o "Sam Spade". Estos programas o comandos muestran la información disponible sobre el dominio consultado. Con esto logramos obtener información sobre:

>>El nombre del administrador

>>Cuándo fue creado y actualizado el registro

>>Los servidores DNS primarios y secundarios

>>Los dominios asociados al de la empresa.

Después de haber identificado todos los dominios asociados, comenzará a consultar los DNS. El DNS es una base de datos

```
[bash]$ whois "empresa."@whois.crsnic.net
[whois.crsnic.net]
Whois Server Versión 1.1

Domain Names in the .com, .net, and .org domains can
now be registered with many different competing regis-
trars. Go to http://www.internic.net for detailed in-
formation.

empresa-travel.com
empresa.net
empresa.org
empresas.com

Con el comando whois, si ponemos un "." al final del
dominio a consultar, se
listarán todos los dominios que comiencen con el nombre
de la empresa.
```

Con el comando whois, si ponemos un "." al final del dominio a consultar, se listarán todos los dominios que comiencen con el nombre de la empresa.

distribuida que se utiliza para transformar las direcciones IP en los nombres de host, y viceversa. Si un DNS está configurado de forma insegura, es posible obtener información muy relevante sobre la empresa. El comando "nslookup" es la herramienta más popular para realizar dicha tarea.

```
[bash]$ nslookup
Default Server: dns2.acme.net
Address: 10.10.20.2

>> server 10.10.10.2

Default Server: [10.10.10.2]
Address: 10.10.10.2

>> set type=any
>>    ls    -d    Acme.net.    >>
/tmp/zone_out
```

Una vez identificadas las redes potenciales, podrá intentar determinar su topología, así como sus rutas de acceso potenciales.

Para esto, existe una herramienta llamada "traceroute" que nos permite seguir un paquete IP desde un host al siguiente. Es decir, analiza la ruta que sigue un paquete dentro de una determinada red, y así permite detectar redes activas, filtrador de paquetes o firewalls.

Existen infinidad de herramientas en Internet que facilitarán información

Es posible que en un entorno gráfico, como el VisualRoute, que no solo proporciona información de las rutas, sino que también la localización geográfica.

Herramientas

Existen infinidad de herramientas en Internet que facilitarán información o ayudarán a encontrar lo buscado. En la siguiente tabla enumeramos alguna de ellas con sus respectivas páginas web.

Contramedidas

Hemos visto las técnicas y herramientas de footprinting. Existen muchas contramedidas. Por ejemplo muchos programas y herramientas comerciales permiten la detección de intrusos en la red (llamado Network Intrution Detection Systems) NIDS.

Quizás uno de los mejores es gratuito: SNORT (www.snort.org) de Marty Roesch al cual dedicaremos uno de nuestros artículos. Humble de Rhino9 ha desarrollado un programa llamado RotoRouter (http://packetstorm.security.com/UNIX/loggers/rr-1.0.tgz . Este le permitirá registrar las solicitudes del traceroute generando respuestas falsas.

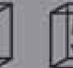
Siempre podrá configurar sus routers frontera limitando el tráfico ICMP y UDP.

Sam Spade.org



ARIN database	http://www.arin.net/whois/
Cyberarmy	http://www.cyberarmy.com
Dogpile (meta search engine)	http://www.dogpile.com
DomTools (axfr)	http://www.domtools.com/pub/domtools1.4.0.tar.gz
Ferretsoft	http://www.ferretsoft.com
Sam Spade	http://www.samspade.org
Securities and Exchange Commission (SEC)	http://www.sec.gov/
USENET Searching	http://www.deja.com http://www.dogpile.com
VisualRoute	http://www.visualroute.com
WHOIS database	http://www.networksolutions.com
WS_ Ping Pack Pro	http://www.ipswitch.com




Paso 2 : Scanning

Escaneo de puertos

Footprinting permite obtener información, entre otras cosas, sobre rangos de direcciones IP, servidores DNS y servidores de e-Mail. Con esta información en nuestro poder, ya es posible determinar que sistemas están "vivos"

Introducción

Hemos visto que, aplicando la técnica de footprinting se puede obtener una lista de direcciones IP correspondientes a hosts y redes usando los utilitarios whois y nslookup. Estas herramientas nos permiten obtener información, entre otras cosas, sobre rangos de direcciones IP, servidores DNS y servidores de e-Mail. Con esta información en nuestro poder, ya es posible determinar qué sistemas están "vivos" (encendidos) y alcanzables desde internet utilizando una variedad de herramientas que incluyen ping sweeps (barridos de ping), port scans (escaneos de puertos), detección de Sistemas Operativos y automated discovery (descubrimiento automatico).

```
woody:~# nmap -sP 192.168.0.1-254

Starting nmap 3.55 ( http://www.insecure.org/nmap/)
Host 192.168.0.1 appears to be up.
Host 192.168.0.2 appears to be up.
Host 192.168.0.3 appears to be up.
Host 192.168.0.4 appears to be up.
Host 192.168.0.5 appears to be up.
Host 192.168.0.7 appears to be up.
Host 192.168.0.8 appears to be up.
Host 192.168.0.11 appears to be up.
Host 192.168.0.21 appears to be up.
Host 192.168.0.41 appears to be up.
Host 192.168.0.51 appears to be up.
Host 192.168.0.123 appears to be up.
Host woody (192.168.0.210) appears to be up.
Nmap run completed -- 254 IP addresses(13 hosts up)
woody:~#
```

Figura 1 - Resultado de ICMP ping sweep con nmap

Ping Sweeps

Uno de los pasos más importantes en el trazado de un mapa esquemático de una red es realizar un barrido de ping sobre rangos de direcciones IP y/o bloques de red para determinar cuales sistemas están "vivos". Este paso se realiza con herramientas que permiten hacer la misma tarea que el rudimentario ping, es decir enviar un ICMP Echo (Tipo 8) al posible destinatario y esperar obtener un ICMP Echo_Reply (tipo 0), determinando así que el posible destinatario esta "vivo".

Aunque existen muchas herramientas disponibles en el mercado, en este artículo nos concentraremos en el uso de nmap, una poderosísima herramienta desarrollada por Fyodor (http://www. insecure. org/nmap). En la Figura 1 vemos la sintaxis para realizar un barrido de direcciones IP utilizando el protocolo ICMP.

El modificador -s permite determinar el tipo de escaneo que se va a realizar (en la Figura 1, la P adicional indica a nmap que haga un ping scan); las direcciones IP de los posibles destinatarios se pueden especificar individualmente ó utilizando rangos en cualquiera de los octetos (como en la Figura 1), también se pueden especificar bloques de red (usando por ejemplo: 192.168.0.0/24 ó 192.168.0 - 12.0/25). Cuando se hace un barrido de direcciones IP utilizando el protocolo ICMP, hay que hacer todo lo posible por evitar las direcciones de broadcast (difusión), debido a que estas direcciones tienden a producir DoS (Denial of Service-Negacion de Servicio).

El primer problema que se puede presentar, al hacer un barrido de direcciones IP utilizando el protocolo ICMP, es que este protocolo esté bloqueado en un router o firewall en el borde de una DMZ (De-Militarized Zone - Zona DesMilitarizada). Aquí es necesario hacer un barrido de direcciones utilizando otro protocolo y/o evaluando ciertos puertos conocidos de los posibles destinatarios del barrido. En la Figura 2 vemos la sintaxis para realizar un barrido de direcciones IP sin utilizar el protocolo ICMP.

El modificador -s permite determinar el tipo de escaneo que se va a realizar (en la Figura 2, la P adicional indica a nmap que haga un ping scan); pero el modificador PT80 le dice a nmap que haga un TCP

Figura 2 - Resultado de TCP probe scan con nmap

```
woody:~# nmap -sP -180 192.168.0.1-254

Starting nmap 3.55 ( http://www.insecure.org/nmap/)
Host 192.168.0.1 appears to be up.
Host 192.168.0.2 appears to be up.
Host 192.168.0.3 appears to be up.
Host 192.168.0.4 appears to be up.
Host 192.168.0.5 appears to be up.
Host 192.168.0.7 appears to be up.
Host 192.168.0.8 appears to be up.
Host 192.168.0.12 appears to be up.
Host 192.168.0.21 appears to be up.
Host 192.168.0.31 appears to be up.
Host 192.168.0.41 appears to be up.
Host woody (192.168.0.210) appears to be up.
Nmap run completed -- 254 IP addresses(12 hosts up)
woody:~#
```

probe scan. Así, utilizando el protocolo TCP sobre el puerto 80, se logra que el barrido supere un posible router y/o firewall debido a que muy probablemente el tráfico sobre el puerto 80 del protocolo TCP este permitido.
Como se puede ver, esta técnica es muy efectiva para superar el escollo del bloqueo del tráfico ICMP. También vale la pena reintentar el mismo rango de direcciones utilizando diferentes puertos de protocolos conocidos, por ejemplo: FTP (21) SMTP (25), POP3 (110), RPCBIND (111), IMAP (143), MSRPC (135).

Ping Sweeps - Contramedidas

El proceso de detección de un Ping Sweep es crucial para determinar si va a ocurrir un ataque, cuándo va a ocurrir y quién lo va a realizar. El principal método de detección de un Ping Sweep es utilizar un NIDS (Network-based Intrusion Detection System-Sistema de Detección de Intrusos basado en Red).

Mientras que la detección de los Ping Sweeps es crítica, la prevención también hará una contribución substancial.

Es recomendable que evalúe el tipo de tráfico ICMP que permite circular en su red. Recuerde que existen 18 (dieciocho) tipos distintos de tráfico ICMP, Echo y Echo_Reply son sólo 2 (dos) de ellos.

Port Scanning

Hasta aquí hemos visto cómo se puede determinar que sistemas están "vivos", utilizando las técnicas de Ping Sweep ó de TCP Probe Scanning. Habiendo recolectado esta información, ya es posible hacer un Port Scanning (Escaneo de Puertos) sobre cada equipo/sistema individual. Port Scanning consiste en establecer conexiones TCP y UDP a un equipo de destino (una posible "víctima") para establecer qué servicios están en ejecución o en estado Listening (escuchando). Los servicios activos que estén escuchando pueden permitir el acceso no autorizado a usuarios no deseados. Estos usuarios podrían lograr acceso a servidores que están mal configurados o que tienen instaladas versiones de aplicaciones que tienen vulnerabilidades conocidas.

Existen varios tipos de escaneo de puertos, dando una perspectiva distinta de cómo detectar servicios

Port Scanning - Tipos de Scan

Existen varios tipos de escaneo de puertos, dando una perspectiva distinta de cómo detectar servicios y/o aplicaciones.

Asimismo, los diferentes tecnicismos de cada uno de ellos permitirá hacer los escaneos con un mayor o menor grado de sigilo.

>>TCP connect scan: este tipo de scan se conecta al puerto de destino haciendo un Three-Way Handshake completo. (Pasos 1, 2 y 3 de la Figura A de la pastilla)

>>TCP SYN scan: esta técnica es conocida también como "half-open scanning", debido a que solamente se envia un paquete con el flag SYN a la "víctima", si ésta responde con un flag SYN/ACK el puerto está escuchando, si responde con un flag RST/ACK el puerto está cerrado. Para evitar el Three-Way Handshaking, se envía un paquete con el flag RST/ACK, y así se logra que la "víctima" no registre una conexión.

```
woody:~# nmap -O 192.168.0.21

Starting nmap 3.55 ( http://www.insecure.org/nmap/ )
Interesting ports on 192.168.0.21:
(The 1643 ports scanned but not shown below are in state: closed)
PORT      STATE   SERVICE
9/tcp     open    discard
13/tcp    open    daytime
 .
 .
901/tcp   open   samba-swat
933/tcp   open   unknown
9999/tcp open   abyss
MAC Address: 00:08:54:06:16:DB (Netronix)
Device type: general purpose
Running: Linux 2.4.X12.5.X12.6.x
OS details: Linux 2.4.0 - 2.5.20. Linux 2.4.18 - 2.6.4. (x86)

Nmap run completed -- 1 IP address (1 host up)
woody:~#
```
Figura 3 - Resultado de TCP SYN scan con nmap

>>TCP FYN scan: con esta técnica se envía un paquete con el flag FIN a la "víctima", y está debe responder un paquete con el flag RST para los puertos que estén cerrados.

>>TCP Xmas Tree scan: con esta técnica se envía un paquete con los flags FIN, URG y PUSH a la "víctima", y ésta debe responder un paquete con el flag RST para los puertos que estén cerrados.

>>TCP Null scan: con esta técnica se envía un paquete que tiene todos los flags apagados a la "víctima", y esta debe responder un paquete con el flag RST para los puertos que estén cerrados.

>>UDP scan: con esta técnica se envía un paquete a un puerto específico de la "víctima", y ésta debe responder un paquete ICMP Port_Unreachable para los puertos que estén cerrados. Los únicos problemas de esta técnica son: su falta de fiabilidad y su baja performance.

En la Figura 3 podemos ver a nmap haciendo un TCP SYN scan sobre uno de los destinos "vivos" de la red.

El modificador -s permite determinar el tipo de escaneo que se va a realizar (en la Figura 3, la S adicional indica a nmap que haga un TCP SYN scan); es posible especificar el FQDN de la "victima", pero es preferible usar su dirección IP.

Las direcciones IP de los posibles destinatarios se pueden especificar individualmente ó utilizando rangos en cualquiera de los octetos (como en la Figuras 1 y 2, pero hay que hacer todo lo posible por evitar las direcciones de broadcast (difusión).

Para los demás tipos de escaneo es necesario usar una T (TCP connect scan), F (TCP FIN scan), X (TCP Xmas Tree scan), N (TCP Null scan) ó U (UDP scan).

Si agregamos el modificador V (resultando en -sSV) nmap tratará de informarnos de la versión de la aplicación y/o servicio que está escuchando en ese puerto.

La cantidad de modificadores que tiene nmap y sus posibles combinaciones hacen imposible que lo mostremos en este artículo.

Existen además otras herramientas disponibles, un ejemplo es la herramienta portqry de Microsoft. Es

gratuita y se puede buscar y bajar del Knowledge Base del sitio de Microsoft (www.microsoft.com). Otro ejemplo es netcat o nc, escrita por Hobbit, (http://www.atstake.com research/tools/network_utilities) que se ha ganado el apodo "TCP/IP Swiss Army Knife", ya que puede cumplir una gran variedad de funciones.

Port Scanning - Contramedidas

El principal método de detección de un Port Scanning es utilizar un HIDS (Host-based Intrusion Detection System-Sistema de Detección de Intrusos basado en Sistemas Individuales). También es posible utilizar un NIDS con su placa de red configurada en modo promiscuo.
De la misma manera que la prevención ayudaba a evitar los Ping Sweeps, la correcta configuración y mantenimiento de los routers y/ó firewalls hará que sea más difícil que un intruso conozca los puertos/servicios/aplicaciones abiertos en los sistemas que se estén asegurando.

Detección de SO

Si prestamos atención a las respuestas que dio nmap al TCP SYN scan, podemos interpretar esos datos y deducir, siguiendo algunas premisas conocidas, que la máquina "víctima" tiene alguna clase de sistema operativo Windows (debido a los puertos 135 y 139 abiertos). Pero muchas veces, los puertos abiertos en un sistema no son fáciles de deducir y producen incertidumbre. Aquí entra en juego nuevamente nmap que nos permite mediante el modificador -O identificar

```
woody:~# nmap -sP -PT80 192.168.0.1-254

Starting nmap 3.55 ( http://www.insecure.org/nmap/ )
Host 192.168.0.1 appears to be up.
Host 192.168.0.2 appears to be up.
Host 192.168.0.3 appears to be up.
Host 192.168.0.4 appears to be up.
Host 192.168.0.5 appears to be up.
Host 192.168.0.6 appears to be up.
Host 192.168.0.7 appears to be up.
Host 192.168.0.8 appears to be up.
Host 192.168.0.12 appears to be up.
Host 192.168.0.21 appears to be up.
Host 192.168.0.31 appears to be up.
Host 192.168.0.41 appears to be up.
Host woody (192.168.0.210) appears to be up.
Nmap run completed -- 254 IP addresses (12 hosts up)
woody:~#
```

Figura 4 - Resultado de detección de SO con nmap

de acuerdo al fingerprint del stack TCP cuál es el sistema operativo de la "víctima". Vemos en la Figuras 4 un ejemplo de detección de sistema operativo. También existen otras herramientas disponibles para la detección de sistemas operativos, un ejemplo muy conocido es QueSo.
(QueSo www.apostols.org/projectz/).
Es importante recordar que QueSo no es un Port Scanner, solamente hace detección de sistema operativo a través del puerto TCP:80.

Detección de SO - Contramedidas

Debido a que el proceso de detección de Sistema Operativo de una máquina "víctima" es esencialmente un análisis del fingerprint del stack TCP, las herramientas para evitar ésta técnica son las mismas que para evitar un Port Scanning: HIDSs y NIDSs.

Descubrimiento automático

Existen herramientas muy completas diseñadas para englobar varias funcionalidades en el scanning. Mencionaremos dos:
i) Cheops que engloba usando una interfaz gráfica a ping, traceroute, port scanning, y scanning de SOs. (http://www.marko.net /cheops/) .
ii) Tkined (parte del paquete Scotty, (http://www.home.cs.utwente.nl /~schoenw/scotty/).

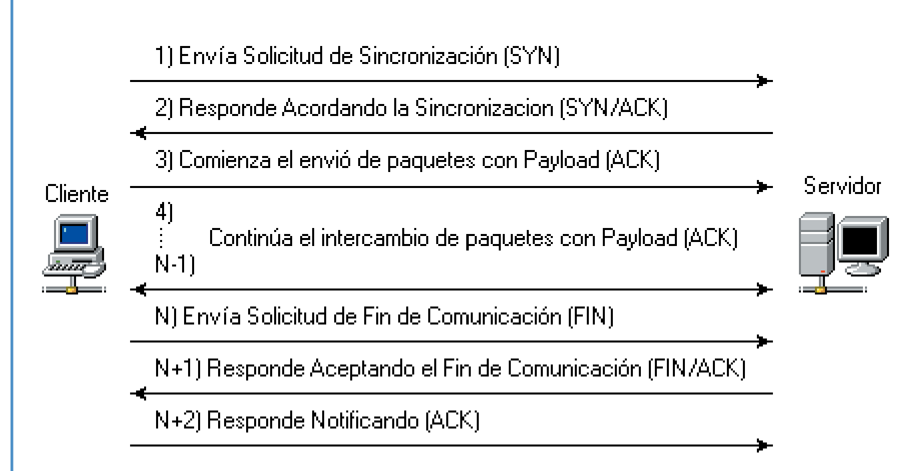
Conclusión

Hemos visto hasta aquí las principales herramientas y técnicas de scanning existentes, la información que es posible obtener y la utilidad de dicha información.
Como postre a nuestro banquete de herramientas y técnicas, sólo queda nombrar una herramienta que permite hacer todas estas tareas en conjunto y desde una única interfaz: Nessus (www.nessus.org), una herramienta que consta de 2 partes, el Server está disponible sólo para plataformas Unix y/o Linux y el cliente està disponible para cualquier plataforma. El cliente funciona en modo gráfico.

Three Way Handshaking

En toda comunicación TCP/IP, así como en la vida real, existen 2 (dos) interlocutores, de aquí en más llamaremos "cliente" al que inicia la comunicación y "servidor" a quien recibe y contesta la comunicación.

Cuando un cliente necesita comunicarse con un servidor, lo hace con algún servicio que está en ejecución en ese servidor. Así el cliente no sólo debe conocer la dirección IP del servidor, sino que también debe conocer el puerto donde este servicio está "escuchando".



En todo paquete TCP/IP, en el header (encabezado) del paquete, están la dirección IP y puerto de origen, la dirección IP y puerto de destino y un flag (bandera de estado) que establece el tipo de paquete. El estado de este flag tiene como propósito establecer un three way handshaking (saludo de 3 vías) para luego dar paso a un intercambio fluido de paquetes.

En la siguiente figura podemos ver un esquemático de este proceso de Three-Way Handshaking. Claramente puede verse que el intercambio de paquetes para acordar la finalización de la comunicación responde al mismo criterio de Tree-Way Handshaking.

Paso 3: Enumeración

Identificación de recursos

La técnicas de enumeración serán específicas de cada sistema operativo.

Si el hacker logró identificar su objetivo (footprinting y scanning), intentará identificar recursos de red, cuentas de usuario y aplicaciones que brinden servicios. A esto se lo denomina "enumeración" y es el paso previo al hackeo. En este artículo veremos enumeración en detalle.

Introducción

Hemos visto las dos primeras acciones que realizará un hacker: "footprinting" y "scanning". Lo que habrá logrado es identificar su objetivo (su número IP, nombre de máquina, dominio de Internet al cuál pertenece) y conocer los puertos que tiene "activos" y su sistema operativo.

```
c:>> Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>nbtstat -A 192.168.0.22


        NetBIOS Remote Machine Name Table

      Name                   Type          Status
   ---------------------------------------------
   MAQ-81             <00>  UNIQUE       Registered
   MAQ-81             <20>  UNIQUE       Registered
   WORKGROUP          <00>  GROUP        Registered
   WORKGROUP          <1E>  GROUP        Registered
   MAQ-81             <03>  UNIQUE       Registered
   MAQ-81             <64>  UNIQUE       Registered
   INet~Services      <1C>  GROUP    Registered
   IS~MAQ-81......<00>  UNIQUE     Registered
   ADMINISTRATOR  <03>  UNIQUE     Registered


   MAC Address = 00-08-54-04-32-F6
```

Figura 1. Pedido de la tabla de nombres de un sistema remoto usando "nbtstat"

NBSTAT extrae el nombre NETBIOS de la máquina blanco, el dominio en el que se encuentra, cualquier usuario que haya iniciado una sesión , cualquier servicio que se encuentre en ejecución .

El paso siguiente, que describiremos a continuación, se llama "enumeración".

Enumerar significa identificar:

>>Recursos de red (máquinas y dominios) y recursos compartidos

>>Cuentas de usuarios

>>Aplicaciones que estén brindando servicios.

Existe una diferencia importante entre "footprinting" y "scanning" y la enumeración. Esta es el grado de intrusión.

Durante la enumeración haremos una conexión activa a los sistemas. Esto implica que estas intrusiones serán detectadas y quizás registradas (existirá un log (registro del evento) por la víctima. La información que se obtiene durante la enumeración no parecería representar gran peligro. Pero no es así. Conocer el UID (nombre de cuenta de los usuarios) o recursos compartidos o detalles de las aplicaciones que están corriendo es de gran ayuda para los pasos que continúan durante el hackeo de una máquina.

La técnicas de enumeración serán específicas de cada sistema operativo. Por ello, deberíamos dividir este artículo en tres partes: Windows NT/2000-2003, Novell Netware y Unix. Por razones de espacio, nosotros nos concentraremos en Windows y sistemas Unix-like (UNIX, BSD-like y Linux).

SNMP

El nombre corto para "Simple Network Management Protocol", un conjunto de protocolos para manejar redes complejas. La primera versión de SNMP fue desarrollada a comienzos de los '80. SNMP trabaja mandando mensajes, llamados "unidades de datos de protocolo" (protocol data units - PDUs) a diferentes partes de una red. "SNMP-compliant devices" (dispositivos SNMP-compatibles), llamados agentes, almacenan datos sobre ellos mismos en Management Information Bases (MIBs) y devuelven estos datos a los consultantes-SNMP (SNMP-requester).

En este artículo de NEX IT Specialist, vamos a dar una introducción, un panorama global. Destacaremos algunos conceptos muy importantes que es necesario comprender en cada uno de los sistemas operativos.

Puertos activos

Cada puerto "activo" detectado durante el "scanning" significa un servicio. El método de "banner grabbing" (establecer una conexión al puerto activo y obtener un mensaje respuesta) nos dá información sobre qué aplicación está escuchando en ese puerto y detalles de ella (por ejemplo su versión). Con esta información podremos decidir si existe alguna vulnerabilidad asociada.

Podríamos por tanto ir recorriendo los distintos puertos posibles (del 1 al 65535) e ir detallando qué herramientas usar en cada caso y qué información obtendríamos.

En el libro "Hackers Exposed" versión 4 (autores: Stuart McClure, Joel Scambray, George Kurtz, McGraw-Hill Osborne Media; 4 edition (February 25, 2003)) que recomendamos, se desarrolla el tema de enumeración de este modo y resulta muy instructivo. Aquí lo haremos de un modo más ortodoxo. Para cada SO, veremos qué herramientas son apropiadas para cada tipo de enumeración posible.

La Tabla 1 muestra los puertos más comunes a encontrar

activos y las aplicaciones asociadas.

Enumeración de Windows NT / 2000-2003

Desde los tiempos de Windows NT los SOs Windows han permitido a los posibles atacantes obtener mucha información. Esto se ha debido, fundamentalmente a la utilización del protocolo NETBIOS y del CIFS/SMB, utilizados para la compartición de archivos.

Dos grandes debilidades de los SOs Windows.

1. Null session-anonymous login

CIFS/SMB y NETBIOS incluyen APIs (Application Programming Interface) que permiten acceder a mucha información de nuestros sistemas. Particularmente sobre los puertos TCP y UDP 135 a 139 y 445. El modo de acceder a esos APIs es a través del llamado "Null Session" o "Anonymous Login". En esta colección encontrará un artículo detallado sobre esta debilidad y sus contramedidas para NT, W2K, XP y Windows 2003.

Allí podrá ver ejemplificada una de las herramientas más populares de enumeración de cuentas de usuarios: enum.exe.

```
C:\>enum -U -d -P -L -c 192.168.0.12
server: 192.168.0.12
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
opening lsa policy... success.
server role: 3 [primary (unknown)]
names:
  netbios: MAQ-FILESERVER
  domain: WORKGROUP
quota:
  paged pool limit: 33554432
  non paged pool limit: 1048576
  min work set size: 65536
  max work set size: 251658240
  pagefile limit: 0
  time limit: 0
trusted domains:
  indeterminate
netlogon done by a PDC server
getting user list (pass 1, index 0)... success, got
24.
  __vmware_user__ (VMware User)
  attributes:
   Administrator (Built-in account for administering
the computer/domain)
  attributes:
  AFernandez (Profesora de Linux)
  attributes:
  ASPNET (Account used for running the ASP.NET worker
process (aspnet_wp.exe))
  attributes: no_passwd
  BPerez (Profesor Linux)
  attributes:
  Cecilia (Recepcion)
  attributes:
  Charlie (Gerencia General)
  attributes:
  ...
C:\>
```

Figura 2. "enum.exe" en plena acción

2. Windows NT/ 2K-2003 Resource Kit

Windows NT 3.1 y los SOs que siguieron fueron complementados con una serie de herramientas (software y documentación) para ayudar a administrar las redes bajo SOs Windows.

Estas incluyen Perl (un poderoso lenguaje de scripting), y aplicaciones equivalentes a otras del mundo UNIX junto con herramientas de administración remota (lea el artículo Windows Services for Unix (WSFU) en #12 pag 39 de NEX IT Specialist).

Es indispensable para cualquier administrador tener esas herramientas llamadas "Resource Kit": NTRK (NT Resource Kit) para Windows NT y W2RK para Windows 2000. Sumado a esto una cantidad de herramientas muy poderosas son incluidas en los CD de instalación en el directorio Support/Tools.

NETBIOS

Protocolo de red originalmente creado para redes locales de computadoras IBM PC. NetBIOS fue la API del producto llamado "PC Network", desarrollado por Sytec, empresa contratada por IBM. "PC Network" no soportaba más de 80 nodos y era bastante simple, pero en aquella época era más apropiado para los ordenadores personales que su pariente más viejo y complejo para mainframes de IBM, el SNA. NetBIOS engloba un conjunto de protocolos de nivel de sesión, que proveen 3 tipos de servicios:Servicio de nombres, servicio de paquetes,servicio de sesión.
El servicio de nombres permite el registro de nombres de computador, aplicaciones y otros identificadores en general en la red. Un programa puede, a través de este servicio, determinará qué computadora en la red corresponde un determinado nombre.
El servicio de paquetes (en inglés, datagram) es análogo al protocolo UDP y posibilita el envío y recibimiento de paquetes en la red.
El servicio de sesión permite el establecimiento de conexiones entre dos puntos en la red y es análogo al protocolo TCP.
NetBIOS es utilizado por protocolos de nivel más alto como SMB.

NFS (Network File System)

Compartir archivos e impresoras es uno de los servicios de red más fundamentales ofrecidos por los diferentes SOs. Por muchos años, el protocolo de compartición de UNIX ha sido NFS. Este protocolo fue originalmente desarrollado por Sun Microsystems y ha sido implementado en casi todos los sistemas Unix-like.

Cualquier sistema Linux puede actuar tanto como cliente o servidor NFS. Los clientes utilizan el concepto de "montar" (mount) Sistemas de Archivos (File Systems, FS) de servidores NFS a "sus" FSs. Una vez montada la jerarquía de directorios sobre el cliente aparece a los usuarios como un FS local.

Enumeraciones posibles

Detallar todas las posibles enumeraciones posibles sería muy extenso. A continuación se mencionan diferentes herramientas (resaltadas en negrita) que hemos ordenado dependiendo de qué deseamos enumerar y que característica usemos (NETBIOS, SNMP, transferencia de zonas DNS). Seguido a esto, damos tres ejemplos (uno de cada tipo de enumeración) de modo de poder obtener una idea de qué significa enumerar.

1. Enumeración de recursos de red (máquinas y dominios) y recursos compartidos.

a) enumeración NETBIOS






```
c:>> Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>telnet www.itspecialist.com.ar

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Wed, 29 Sep 2004 17:38:18 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head>
</html>

Connection to host lost.
```

Figura 3. "Banner grabbing"

>>De dominios y equipos en el dominio **(netview)**
>>Nombres netbios de sistemas remotos **(nbtstat, nbtscan)**
>>De Domain controlers (**nltest**)
>>Recursos compartidos **(netview, dumpsec, legion).**
>>De servidores tipo ras **(netviewx)**

b) SNMP **(snmputil)**

c) Transferencia de Zona DNS **(nslookup)**

DNS (Domain Name Service),

Es la base de datos distribuida de nombres a números IP. Técnicamente, no es necesario utilizar nombres de host y dominios como www.cortech.com.ar (nombre host www que pertenece al dominio cortech.com.ar). Es el número IP el que necesita el sistema para comunicarse. DNS fue creado para poder usar nombre de dominios y de máquinas y no deber recordar los números IP. Cuando tipeo en mi web-browser: http://www.cortech.com.ar, un pedido sale hacia el servidor DNS que se ha definido de modo que éste me devuelva el IP asociado. Con ese IP se envían los paquetes al servidor web correspondiente.

2. Enumeración de usuarios/cuentas

a) mediante CIFS/SMB

>>**nbtstat** y **nbtscan** (no requiere null session)
>>**dumpsec**
>>**sid2user**, **user2sid** (ver artículo de Mark Russinovich en win2000mag.com artículo #3143)
>>**enum**
>>**nete** (escrita por Sir Dystic del grupo Cult of the Dead Cow)

b) usando SNMP

c) de AD usando cliente **ldp.exe** (está en Support/Tools)

3. Enumeración de aplicaciones

a)
>>**telnet**
>>**netcat** (escrita originalmente por Hobbit (www.avian.org) es llamada la navaja suiza TCP/IP). Fue portado a Windows por Weld Pond cuando pertenecía al Security Group de L0pht). Está considerada la segunda herramienta de seguridad más importante después de nmap. Desarrollaremos un artículo de esta colección)

b)
Mediante obtención del contenido del registry **(regdmp)**

CIFS

El Common Internet File Siystem (CIFS) es la manera más común en que los usuarios de computadoras comparten archivos a través de intranets (redes internas) e Internet. Es el protocolo por default en Windows 2000 para compartir archivos y es una extensión del protocolo SMB (Server Message Block).

CIFS define una serie de comandos usados para pasar información entre computadoras en red. El "redirector" empaqueta consultas para computadoras remota en una estructura CIFS. CIFS puede ser enviado mediante una red a dispositivos remotos. El "redirector" también usa CIFS para hacer consultas al stack del protocolo de la computadora local. Los mensajes CIFS pueden ser clasificados como:

>>mensajes para establecer conexión: consisten en comandos que empiezan y terminan una conexión del "redirector" a un recurso compartido en el servidor.
>>mensajes con manipulación de nombres y archivos son usados por el "redirector" para lograr el acceso a archivos en el servidor y para leerlos y escribirlos.

>>mensajes a las impresoras son usados por el "redirector" para enviar información a una cola de impresión en el servidor y para obtener información sobre su estado.

>> mensajes variados son usados por el "redirector" para escribir a "mailslots" y "named pipes".

Ejemplos:

Ejemplo 1.: Enumeración de los nombres NETBIOS de sistemas remotos

"nbtstat" está incorporada dentro de los sistemas operativos Windows. Usada como se ejemplifica en la figura 1., nos permite obtener la tabla de nombres NETBIOS de un sistema remoto. En este caso la máquina con número IP 192.168.0.22.

Como podemos observar "nbstat" extrae el nombre NETBIOS de la máquina blanco (MAQ-81), el dominio en el que se encuentra (WORKGROUP), cualquier usuario que haya iniciado una sesión (ADMINISTRATOR), cualquier servicio que se encuentre en ejecución (INet-Services). Además nos da el MAC address de la máquina víctima. Notar que hay dos números entre corchetes a la derecha del "name". Estos identifican los tipos de servicios NETBIOS que corren en la máquina.

Ejemplo 2 Enumeracion de usuarios de cuentas

"enum.exe" es una herramienta que unifica todas las funciones de enumeración posibles de realizar sobre NETBIOS. Fue hecha por el equipo Razor de BindView y puede obtenerse en http://razor.bindview.com.

En la figura 2, podemos observar la cantidad de información que podemos obtener cuando la dirigimos a una máquina víctima. Lista políticas de password, nombres NETBIOS y de dominio, usuarios de la máquina y mucha más información que dependerá de qué opciones activemos.

Haciendo sólo "enum" obtenemos una lista de todas sus posibilidades.

En esta colección de Ethical Hacking encontrará "enum.exe" mucho más detallado en el artículo por Carlos Vaughn O´Connor "Entendiendo Null Sessions o Login anónimo".

Ejemplo 3 Enumeración de aplicaciones mediante "banner grabbing"

La Figura 3 nos muestra el "banner" que nos devuelve la máquina víctima al hacer telnet sobre un puerto que sabemos está activo. En este caso vemos que la aplicación es el web-server IIS 5.0 de Microsoft (Internet Information Server 5.0). Si conociésemos alguna vulnerabibilidad del IIS 5.0 podríamos intentar aplicar un exploit sobre la misma.

Enumeración de UNIX.

Los sistemas operativos UNIX, basan todas sus funciones de red bajo TCP/IP. Por tanto la información que proveen es más limitada que la que brinda NETBIOS en el caso Windows. Esto no significa que no existirá la posibilidad de hacer "enumeración" bajo Unix. Sí que es conocido y predecible lo que es posible obtener.

En los recuadros adjuntos detallamos someramente las técnicas de administración de redes usadas más comúnmente bajo UNIX: Remote Procedure Call (RPC), Network Information System (NIS) y Network File System (NFS). La utilización de LDAP como protocolo para Servicio de Directorio (Directory Service) abre también otro mecanismo posible de enumeración.



NIS

El Network Information Service o NIS es un protocolo de servicio de directorio de "páginas amarillas" (YP, yellow pages) cliente-servidor. Fue desarrollado originalmente por Sun Microsystem para configuración de sistemas de distribución de datos como nombres de usuarios y "hostnames" entre computadoras en una red de computadoras. NIS/YP es usado para mantener un directorio central de usuarios, "hostnames" y muchas otras cosas útiles en una red de computadoras. Por ejemplo, en un ambiente UNIX , la lista de usuarios (para autenticación) está situada en /etc/passwd. Usar NIS agrega otra lista de usuario global que es usada para autentificar usuarios en cualquier "host".
Sun licencia esta tecnología para virtualmente todo otro "vendor" de Unix.
Como "páginas amarillas" es una marca registrada en el Reino Unido, de British Telecommunications PLC para su directorio telefónico comercial (en papel), Sun cambió el nombre de su sistema a NIS, aunque todos sus comandos y funciones aún empiezan con "yp".
En ambientes modernos, servicios de directorio como Lightweight Directory Access Protocol (LDAP) y Kerberos han reemplazado a NIS. ya que son considerados más modernos y seguros que NIS.

Lista de puertos más comunes

20 FTP data (File Transfer Protocol)
21 FTP (File Transfer Protocol)
22 SSH (Secure Shell)
23 Telnet
25 SMTP (Send Mail Transfer Protocol)
43 whois
53 DNS (Domain Name Service)
68 DHCP (Dynamic Host Control Protocol)
79 Finger
80 HTTP (HyperText Transfer Protocol)
110 POP3 (Post Office Protocol, version 3)
115 SFTP (Secure File Transfer Protocol)
119 NNTP (Network New Transfer Protocol)
123 NTP (Network Time Protocol)
137 NetBIOS-ns
138 NetBIOS-dgm
139 NetBIOS
143 IMAP (Internet Message Access Protocol)
161 SNMP (Simple Network Management Protocol)
194 IRC (Internet Relay Chat)
220 IMAP3 (Internet Message Access Protocol 3)
389 LDAP (Lightweight Directory Access Protocol)
443 SSL (Secure Socket Layer)
445 SMB (NetBIOS over TCP)
1433 Microsoft SQL Server
1494 Citrix ICA Protocol
1521 Oracle SQL
1604 Citrix ICA / Microsoft Terminal Server
2049 NFS (Network File System)
3306 mySQL
4000 ICQ
5010 Yahoo! Messenger
5190 AOL Instant Messenger
5632 PCAnywhere
5800 VNC
5900 VNC
6000 X Windowing System
6699 Napster
6776 SubSeven (Trojan - security risk!)
7070 RealServer / QuickTime
7778 Unreal
8080 HTTP
26000 Quake
27010 Half-Life

SMB

Server Message Block - (SMB) Un protocolo cliente/servidor que provee compartición de archivos e impresoras entre computadoras. Además SMB puede compartir puertos y abstracciones de comunicaciones como "named pipes" y "mail slots". SMB es similar a "remote producer call" (RPC) pero e-specializado en acceso a sistemas de archivo.

SMB fue desarrollado por Intel, Microsoft e IMB a comienzos de los '80. También tuvo influencia de Xerox y 3Com. Es el método nativo de compartición de archivos e impresoras para sistemas de operación de Microsoft, donde es llamado Microsoft Networking. Windows for Workgroups. Windows 95 y Windows NT todos incluyen clientes y servidores SMB. SMB es usado también por OS/2, Lan Manager y Banyan Vines. Hay servidores y clientes SMB para Unix, por ejemplo Samba y smbclient.

SMB es un protocolo de la capa de presentación, estructurado como un gran conjunto de comandos (Server Message Blocks). Hay comandos para apoyar la compartición de archivos, la compartición de impresoras, la autenticación de usuarios, el "browsing" de recursos, y otras funciones variadas. Como muchos clientes y servidores pueden usar diferentes versiones ("dialectos") del protocolo, negocian antes de empezar la sesión.
El "redirector" empaqueta consultas SMB en una estructura de bloque de control (NCB) que puede ser enviada a través de la red a un dispositivo remoto.

SMB originalmente funcionaba encima de los protocolos NetBEUI y NetBIOS, pero ahora funciona normalmente sobre TCP/IP.

Microsoft desarrolló una versión extendida de SMB para Internet, el Common Internet File System (CIFS), que en muchos casos reemplaza a SMB. CIFS funciona sólo sobre TCP/IP.

SAMBA: SMB y NMB (www.samba.org)

El mecanismo de compartición de archivos usado por Microsoft e IBM., llamada Srerver Message Block (SMB) ha sido implementado como Open Source como un suite de programas que se llaman colectivamente SAMBA.
SMB: maneja compartición de archivos e impresoras
NMB: implementa WINS (Windows Internet Name Service), que permite traducir nombres de NETBIOS de máquinas a números IP.

Enumeraciones posibles

Al igual que en el caso de SOs Windows detallar todas las posibles herramientas de enumeración está fuera de lo que haremos aquí. Solo mencionaremos algunas por completitud agrupadas por el tipo de enumeración que permiten (resaltadas en negrita) y daremos un ejemplo.

```
debian[root$]showmount -e 192.168.0.9
export list for 192.168.0.9
/pub                    (everyone)
/usr                    user
/libros                 lectores
```

Figura 4

Si hemos detectado que una máquina tiene el puerto activo 2049, significa que está compartiendo directorios bajo NFS.

1.Enumeración de recursos compartidos y de red

>>showmount

2.Enumeracion de usuarios

>> finger, rwho, rusers, telnet, tftp (trivial ftp)

3.De aplicaciones mediante "banner grabbing"

>> pcinfo, nmap

RPC (Remote Procedure Call)

Los servicios de RPC (Remote Procedure Call) son un conjunto de servicios desarrollados por Sun para permitir la interacción de varias máquinas en una red. Los protocolos de comunicación son públicos, lo que permite que la mayoría de los servicios se implementen sobre distintos sistemas operativos. Este un elemento esencial para la interoperabilidad. Los servicios de RPC tienen un punto en común: la utilización de un portmapper. Se trata de un servicio similar a inetd. Sin embargo, si bien inetd tiene puertos fijos para cada servicio, este no es el caso de RPC. Los servicios RPC son registrados en el portmapper, que les ofrece un puerto cuando lo necesitan. Cuando una maquina necesita un servicio RPC, esta se contacta con el portmapper que ejecutara el servicio e informara al cliente a que puerto debe dirigirse.

4.Enumeración SNMP

>>snmpwalk

Si hemos detectado que una máquina (con número IP 192.168.0.9) tiene el puerto activo 2049, significa que está compartiendo directorios bajo NFS.

Usando el comando "showmount" con la opción -e como se muestra en la figura 4, obtendremos un listado de los recursos que comparte esa máquina.
Este es el comportamiento normal de NFS. Solo deberemos asegurarnos de que los recursos que se comparten tengan los permisos correspondientes de lectura y escritura (read o write).

Paso 4: Hacking NT, 2K, 2003.

Parte 1 de 2

Los sistemas operativos Windows han sido el blanco preferido de las actividades de los hackers. Existen varias razones. En lo que sigue analizaremos el porqué de esto y mostraremos las metodologías y herramientas que se utilizan al momento de comprometer nuestros sistemas y redes. Esto nos enseña cómo defendernos.

Indice

Ya hemos recorrido:

Paso 1: Footprinting
Paso 2: Scanning
Paso 3: Enumeración

Lo primero que debemos comprender es que cualquier hacker buscará tener privilegio de Administrador o System. Una vez obtenidos estos es el dueño absoluto.

Poder acceder a una cuenta de usuario común sólo le sirve al hacker para luego realizar lo que se denomina "escalada de privilegios".

Es decir, el target del hacker es tener los privilegios de ADMINISTRADOR. Dueño absoluto, robará cuanta información encuentre y finalmente esconderá sus huellas. Si le interesase volver en un futuro, instalará los llamados backdoors o preparará todo para permitirle acceso remoto.

En este artículo estudiaremos las metodologías, las vulnerabilidades conocidas y las herramientas que se pueden utilizar para comprometer sistemas y redes completas.

A menos que ya conozca del tema, le recomendamos complementar con la lectura de los artículos relacionados a cuentas de usuarios y passwords en Fundamentos de seguridad Informática de esta colección: "El gran debate pass phrases versus passwords", "Kerberos", "Entendiendo Null Sessions o Login anónimo", "Rainbowcrack : "la herramienta" para crackear los passwords de los sistemas operativos Windows"

PARTE 1

1. Introducción

Los sistemas operativos Windows conforman gran parte de los sistemas de la mayoría de la redes en las empresas. Esta popularidad los ha hecho blanco de las actividades de hacking en los últimos años.

Desde 1997 en que Hobbit publicó un artículo sobre las vulnerabilidades (ver nota en este artículo) en NETBIOS /CIFS/SMB y LM (los protocolos sobre los que los sistemas Windows basan su conectividad, compartición de archivos, y autenticación) el número de "exploits" ha sido muy grande.

Microsoft ha sistemáticamente corregido las vulnerabilidades encontradas y los nuevos sistemas operativos Windows han logrado una madurez, siempre que estén bien configurados.

Mencionemos solamente las mejoras que Windows 2000 /2003 trajo sobre Windows NT: IPsec, EFS, Group Policies, Security Templates, RADIUS y autenticación Kerberos.

Quizás uno de los factores que hacen más difícil resolver muchos problemas, es la necesaria compatibilidad con sistemas operativos llamados legacy (DOS/Windows 1.x/3.x/9x/Me).

Otro factor, viene pegado al hecho de ser muy fáciles de usar y contener muchas aplicaciones. La simplificación en el uso del sistema operativo también hace sencillo el uso de herramientas para atacarlo. La gran cantidad de aplicaciones que trae por default amplía el número de posibles vulnerabilidades a encontrar.

Tanto en los medios como en la ficción se obtiene la idea de que la mayoría de los ataques son externos a las redes de las empresas.

Esto no es así. La mayoría de los ataques son conducidos por gente dentro de la empresa y que tienen acceso a la red.

Realizados los paso de footprinting, scanning y enumeración (que describimos en los pasos 1 a 3) el hacker pasará a intentar comprometer (hackear) el sistema (computadora) elegido.

Para esto existen diferentes herramientas que automatizan la acción (algunas son comerciales y otras pueden bajarse de Internet).

En este artículo, describiremos más las ideas básicas y algunas herramientas como ejemplos de modo de poder entender el"big picture" de este tema. No daremos detalle de cada herramienta disponible (que son muchas).

Aquel interesado las podrá encontrar por ejemplo bien descriptas en la 4ta edición de "Hackers Exposed" (Mc Graw Hill- Osborne, www.hackingexposed.com) (si compra la versión en español le advertimos que la traducción es paupérrima).



El hacker, muy probablemente comprometerá primero una máquina no muy crítica (por ejemplo usada como desktop) en la organización y una cuenta de un usuario común. Este será un ataque No autenticado.y el primer escalón. El segundo, será hacer lo que se denomina "escalada de privilegios". Aquí realizará ya un ataque autenticado. Intentará obtener la cuenta ADMINISTRATOR de la máquina conquistada. Si logra esos privilegios muy probablemente, desde esa máquina, intentará proyectarse a servidores más importante (hará sondeos y robos en la red , en inglés "pilfering") hasta finalmente lograr hackear el total de la empresa. Dejará posibilidades de acceder en forma remota y back doors para visitas futuras o redireccionará puertos. El muy experto, logrará borrar sus huellas de modo de que nadie advierta su conquista.

2. Ataques NO autenticados

A. Debilidades de SMB /CIFS

a) PASSWORD GUESSING

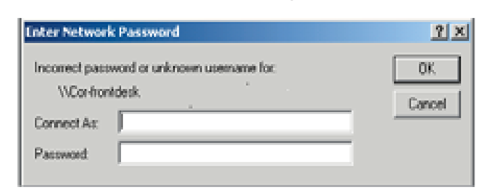
GUESS en inglés significa "adivinar".

Uno puede sentarse frente a una máquina y comenzar a adivinar UID (nombre de usuario) y su password. A menos que tengamos una suerte increíble este proceso es muy improbable de conducir al éxito.

Pero, si el servicio NETBIOS session con su puerto TCP 139 están activos, podré ver recursos compartidos en la máquina victima desde otra máquina simplemente haciendo en Start->run

\\192.168.1.6\IPC$ (recordar que IPC$, C$ o ADMIN$ por ejemplo son recursos compartidos "hidden" casi siempre expuestos en Windows).

Esto nos traerá la GUI siguiente:



Allí podremos probar nuestra suerte nuevamente tipeando.

Por supuesto, este ejercicio se simplificaría si ya conociésemos el UID. Es decir nombres de cuentas de usuarios.

En los paso a paso anteriores (en la enumeración por ejemplo) hemos visto que gracias a las "null sessions" y mediante el comando de línea "net use" era posible obtener la lista de usuarios de la máquina. También existen herramientas completas para hacer esto. Netcat, DumpACL, DumpSec de Somarsoft Inc. y sid2user o user2sid de E. Rudnyi. Conocido el UID sólo queda adivinar la contraseña.

Equivalente a lo anterior es usar el comando net use en el cmd prompt como se muestra en la figura 1

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>net use \\192.168.7.18\IPC$ * /user:Administrator
Type the password for \\192.168.7.18\IPC$:
```

Figura 1.

¿Pero es posible automatizar este proceso de "adivinar" los passwords?. Sí, empleando el comando FOR en el comand prompt.

Podemos generar un archivo con nombres de usuario s y contraseñas que pediremos desde el command prompt como muestra la figura 2.

Lo que pedimos es que se analice el archivo uidpass.txt y extraer los primeros 2 elementos de cada línea. El primero queda el %i y el segundo en %j. net use usará entonces las variables %i y %j

```
archivo uipass.txt

usuario1    ted
usuario2    pepe
```

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.


C:\>FOR /F "tokens=1,2*" %i in (uidpass.txt)
         do net use \\192.168.0.8\IPC$ %i /u:%j

C:\>net use \\192.168.0.8\IPC$ ted /u:usuario1
System error 1219 has occurred.

The credentials supplied conflict with an existing set of credentials.


C:\>net use \\192.168.0.8\IPC$ pepe /u:usuario2
System error 1219 has occurred.

The credentials supplied conflict with an existing set of credentials.
```

Figura 2.

Existen numerosos programas especiales que pueden realizar esta acción automatizada:

De costo cero Legion y NAT (NetBIOS Auditing Tool), NTInfoScan.

CyberCop Scanner de Network Associates Inc. que incluye la utilidad SMBGrind

Como evitar adivinanza de passwords

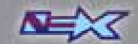
Si nuestra máquina no cumple funciones de file server y es un host de Internet lo más conveniente es bloquear el acceso a los puertos TCP y UDP 135-139 en el firewall o router de nuestra red. También desactivar WINS.

También podremos setear una serie de acciones relacionadas a los passwords. Bloqueo de cuentas después de un número fallido de intentos, forzar políticas de passwords a nivel de empresa y exigidas a cada usuario de modo que cumplan ciertos requisitos. Por ejemplo, la figura 3 nos muestra la GUI donde se setean estos parámetros en W2K.

Existen 2 herramientas passfilt y passprop que debemos discutir en este contexto:

Passfilt: fuerza políticas de passwords fuertes. Viene instalado por default en W2K, pero no está habilitado. Si lo activamos servirá para exigir cierto nivel de passwords en la empresa.

Passprop: Recordemos que la cuenta del administrador es lo más buscado por el hacker. Esta cuenta (RID 500) no se puede bloquear por defecto, de modo que un atacante podrá probar passwords en forma indefinida sin que la cuenta se bloquee. Passprop, es una herramienta que viene con el REsource Kit de los sistemas operativos Windows y nos



permite que se pueda realizar el bloque de ADMINISTRATOR.

Auditoria y event logs. Los sistemas operativos Windows producen logs (registros) de muchas acciones: Application logs, System logs, security logs. Además es posible activar auditorías. Simplemente habilitando las auditorías no es suficiente. Uno debe examinar regularmente los logs buscando evidencias de intrusión. Analizar los logs manualmente puede ser muy tedioso. Pero, la herramienta Event Viewer nos permite filtrar por día, tipo, fuente, categoría, usuario, computadora y ID del evento.

Existen infinidad de herramientas en Internet que nos facilitarán información

IDS (Intrusión Detection System) Sistema de Detección de Intrusos: Un sistema de detección de intrusos o IDS es una herramienta de software empleada para detectar el acceso no autorizado a un sistema de computación o a una red de computadoras. Nos dá la capacidad de alerta en tiempo real. Referimos al lector al artículo "IDS (Intrusión Detection System)" de esta colección.

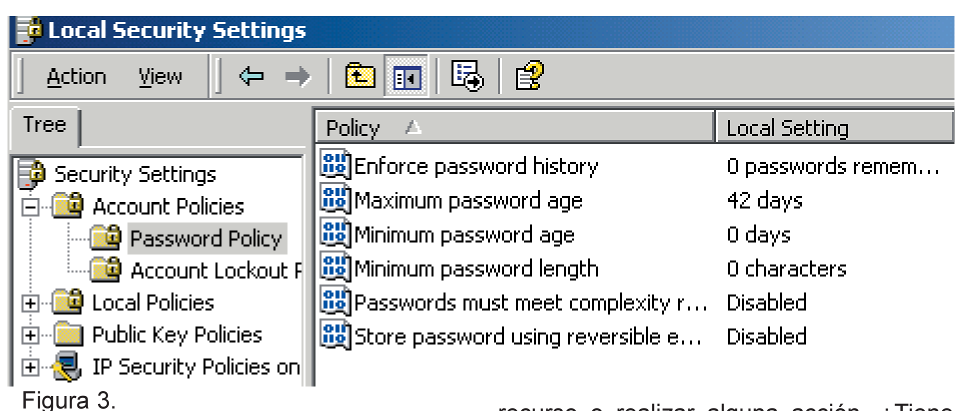


Figura 3.

b) ESPIANDO EN LA RED LOS PASSWORDS: L0phtcrack

Adivinar los passwords es tarea dificil. Casi diríamos imposible de hacer si el administrador tomó recaudos en la elección de los passwords y hubo concientización del manejo de los mismas por parte de los usuarios.
Pero hoy los usuarios y sistemas envían su autenticación a través de la red a los servidores. Un simple programa que sniffee (en inglés " to sniff" significa olfatear y que se entiende como la acción de estudiar y reconocer los paquetes de la red) nuestra red nos dará información de los passwords. Pero, existe una herramienta que hace precisamente esto: L0phtcrack (LC). Entendamos entonces los mecanismos de autenticación de los sistemas operativos Windows, sus debilidades y veamos qué hace LC.

Identificación, Autenticación, Autorización y Responsabilidad (Accountability).

Cuando un sujeto (entendido como un usuario, un programa o un proceso) desea acceder a un recurso, muchas veces se utiliza la palabra "autenticación", englobando cuatro procesos:

Identificación: describe el método de asegurarme que el sujeto existe en la base de datos de los sujetos que pueden acceder a los recursos. Esto se logra tipeando el UID o número de cuenta.

Autenticación: el sujeto debe proveer un segundo elemento identificatorio. Puede ser su password, passphrase, llave criptográfica, un PIN (Personal Identification Number), atributo anatómico o un token.
Estas dos piezas son comparadas con la información almacenada anteriormente en la base de datos sobre este sujeto. Si existe coincidencia el sujeto está identificado y autenticado.

El sujeto ahora intentará acceder a algún recurso o realizar alguna acción. ¿Tiene asignado ese derecho o privilegio? (no todos los sujetos autenticados podrán realizar las mismas acciones ni acceder a los mismos recursos). El sistema buscará en algún tipo de lista, matriz o etiquetas de seguridad que le dirán si está autorizado o no. Este proceso se llama la Autorización (por ejemplo: autorizado a leer información, escribirla, en qué horarios, etc.)

Responsabilidad (Accountability): el sujeto deberá ser responsable de sus acciones. En el sistema que él accede existirán log files y medidas de monitoreo y auditoría donde se registrarán todas las acciones que realice el sujeto.

Instancias de autenticación.

Existen muchas instancias en las que un usuario debe autenticarse en una red. Entre otras:

1. un logon a la red de la empresa
2. cuando accede remotamente a la red de la empresa (dial-up o mediante una VPN a través de Internet)
3. Acceso a un web-server desde su web-browser en una intranet o desde internet.
4. Acceso wireless a un access point.

Cada uno de ellos tiene sus métodos y protocolos de autenticación.

Protocolos de autenticación de acceso a una red (caso 1. del párrafo anterior) bajo sistemas operativos Windows

Los siguientes protocolos son soportados por Windows NT: LAN Manager (LM), NTLM, NTLMv2. Windows 2000-2003 y XP usan Kerberos v5 como el método de autenticación por default si utilizan Active Directory (AD). Ya que es muy posible que en nuestra infrestructura tengamos clientes "legacy" (Windows 95,98 etc) NT, Windows 2000/2003 y XP también soportan las autenticaciones anteriores (LM, NTLM y NTLMv2). Hay que recordar que éstas son autenticaciones más débiles que Kerberos y por lo tanto mucho más sencillas de comprometer.
En cada una de estas metodologías varían la complejidad de los passwords permitidos, el modo de transmitir la información vía la red y dónde y cómo se almacenan las passwords.

Passwords

Las passwords de los usuarios componen uno de los riesgos más grande a la seguridad de las redes. Este riesgo incluye: la creación de las passwords, el modo en que los usuarios las protegen, cómo el sistema operativo las guarda y cómo las password son transmitidas a través de la red.

El sistema operativo es el responsable de guardar y transmitir a través de la red las "credenciales" (nombre de usuario y password) para las cuentas.

Windows 2000/2003 y XP soportan una variedad de distintos protocolos para transmitir las credenciales. También existen una variedad de formas de guardar las credenciales.

Historia de L0phtcrack

Hace unos años The L0pht mostró la debilidad de la autenticación LM de Windows. L0pht introdujo su programa de crackeo de passwords. Y, se transformó en el programa más popular de password-craking del sistema operativo Windows. L0phtcrack LC5 (ver atstake INC., www.atstake.com), es una herramienta administrativa muy respetada y LM ha sido reemplazada por

NTLM, NTLMv2 y Kerberos v5. Pero, hoy LC5 ha sido superado por Rainbowcrack.

Sniffing de nuestra red al autenticarse los sistemas y usuarios.

L0phtcrack incluye una herramienta llamada SMB Packet Capture que nos elimina la necesidad de poseer el archivo dónde se hallan las passwords. Escucha en nuestra red local y captura las sesiones individuales de login entre máquinas que corren WINDOWS. Saca la información pertinente que le exporta al programa principal de L0phtcrack que se encargará de crackear el password.

Recordemos que ahora el tiempo disponible es infinito y no se bloquean las cuentas.!!!!

En un artículo próximo veremos el detalle de cómo funciona L0phtcrack para hallar el password cuando en realidad el hash nunca cruza la red. Recordemos que LM y sus variantes usan una autenticación challenge/response.

En resumen, si puedo sniffear la red por un tiempo suficiente es casi seguro que puedo obtener la cuenta de ADMINISTRATOR en pocos días.
Si tiene dudas de cómo se puede realizar esto en una red switcheada, la respuesta es "técnicas de ARP spoofing" que detallaremos en otro artículo.

La gente de L0pht ha incluso elaborado un sniffer que saca los passwords de WINDOWS de conexiones que usan el protocolo PPTP (Point to Point Tunneling Protocol) en VPNs. (ver http://packetstormsecurity.com/sniffers/ppptp-sniff.tar.gz)

Contramedidas: evitar que la autenticación LM ocurra. Lea un detalle de esto en el artículo: ""Rainbowcrack : "la herramienta" para crackear los passwords de los sistemas operativos Windows" y Pass phrases vs passwords" en esta colección.

B. Ataques sobre IIS

Cuando salió W2K Microsoft IIS 5.0 se instalaba por default. El puerto 80 aparecía abierto y NO todos eran concientes de esto. La explotación por parte de los hacker de vulnerabibilidades utilizando el puerto 80 fueron devastadoras. Windows SERVER 2003 trae IIS 6.0 (una versión corregida) y además el ADMINISTRATOR deberá levantar IIS si así lo desea.

En otro artículo de esta colección analizaremos en detalle WEB SERVER HACKING y WEB APPLICATION HACKING.

COMO SIGUE ESTA HISTORIA (ver PARTE 2)

Supongamos haber podido comprometer un Server W2K, conociendo el uid de un usuario sin privilegios y su passwords. Esto es un logro, pero nuestra objetivo es ser ADMINISTRATOR o que la cuenta tenga los privilegios (es decir pertenecer al grupo de Administradores) de Administrador. A partir de aquí los ataques son autenticados.
El proceso de pasar de usuario común a tener privilegios de Administrador se llama "escalada de privilegios".

Ya obtenidos privilegios de administrador, lo que sigue es lo que llamanos un sondeo y robos para dominar toda la empresa (en inglés se lo conoce como "pilfering"). El paso que sigue será muy probablemente utilizar herramientas para crear los llamados "backdoors" o herramientas de control remoto y redireccionamiento de puertos. Es decir tener a disposición la red cuándo y cómo la desee. NETCAT (llamada la navaja suiza de las herramientas de seguridad, se destaca entre todas y la veremos en detalle en un artículo especial bajo TOOLS. Al igual que un robo sofisticado, el hacker intentará borrar sus huellas como paso final. Su acción ha sido devastadora.

HIDDEN SHARES (recursos compartidos ocultos)

En el SO Windows Server uno encuentra varios "shares"(recursos para compartir) que fueron creados sin nuestra intervención. La mayoría de estos shares son "hidden" (ocultos) y se los nombra con $ al final. Ejemplos: C$.D$, ADMIN$.
Existe un "share" muy particular que debemos entender: IPC$. Es quizás, uno de los shares mas usados en comunicaciones entre servidores. ¿Por ejemplo, cómo leemos los "event logs" en otra computadora?. Uno no mapea un "drive" sino los llamados "named pipes": un pedazo de la memoria que maneja la comunicación entre procesos ya sean locales o remotos

Paso 5: Alguien ha hackeado mi S.O. Windows

Por Carlos Vaughn O'Connor

No es fácil saber si nos han hackeado y menos aún cómo ni quién.

¿Qué hacer?, ¿Cómo abordar el problema? En este artículo le enseñamos dónde buscar los códigos maliciosos que el hacker ha instalado.

Si nuestra máquina (sea una Workstation o server) corriendo un Sistema Operativo Windows ha sido comprometida (se dice también hackeada), muy probablemente estará muy lenta o tendrá una cantidad de tráfico en su placa de red inusualmente grande. En general NO es fácil saber si nos han hackeado y menos aún cómo ni quién.

¿Qué hacer?, ¿Cómo abordar el problema? En este artículo le enseñamos dónde buscar los códigos maliciosos que el hacker ha instalado.
A continuación detallamos tres acciones importantes a seguir:
1. Detectar qué puertos tiene abiertos nuestro sistema víctima y determinar cuáles pueden ser sospechosos.

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    server1:smtp            cor-81:0               LISTENING
  TCP    server1:http            cor-81:0               LISTENING
  TCP    server1:epmap           cor-81:0               LISTENING
  TCP    server1:https           cor-81:0               LISTENING
  TCP    server1:microsoft-ds    cor-81:0               LISTENING
  TCP    server1:1025            cor-81:0               LISTENING
  TCP    server1:1027            cor-81:0               LISTENING
  TCP    server1:1030            cor-81:0               LISTENING
  TCP    server1:1058            cor-81:0               LISTENING
  TCP    server1:1101            cor-81:0               LISTENING
  TCP    server1:1113            cor-81:0               LISTENING
  TCP    server1:1400            cor-81:0               LISTENING
  TCP    server1:3372            cor-81:0               LISTENING
  TCP    server1:3468            cor-81:0               LISTENING
  TCP    server1:4662            cor-81:0               LISTENING
  TCP    server1:6711            cor-81:0               LISTENING
  TCP    server1:6715            cor-81:0               LISTENING


C:\Documents and Settings\Administrator>
```

Figura 1

Recordemos que el hacker pudo haber instalado un "backdoor", un "troyano" o un "Root Kit" que en determinado momento se activa abriendo un puerto y muy posiblemente estableciendo una conexión con nuestro enemigo.

Correr en command prompt:
nestat -a
que nos dice qué conexiones y puertos en escucha tiene nuestra máquina (la víctima).

En la figura 1. vemos una lista de los puertos que aparecen abiertos en un servidor Windows 2000. Por supuesto, otros puertos pueden aparecer abiertos dependiendo de los servicios que tengamos corriendo.
Debemos saber, qué la salida que nos muestra netstat puede estar modificada por el mismo programa que nos hackea. Por eso, debemos correr en forma complementaria, desde otra máquina un scanner de puertos sobre la nuestra. La herramienta más popular es Network Mapper (nmap) de Fyodor (puede ser bajada de www.insecure.org). Existen otras alternativas. Por ejemplo Microsoft sacó una nueva versión de portqry (http://support.microsoft.com/default.aspx?scid=kb;en-us;832919#2, ver tambien los artículos de Mark Minasi sobre el tema.

2. Detectar posibles usuarios NO autorizados

Es muy común que en un sistema hackeado aparezcan usuarios creados por el hacker. Normalmente con privilegios de administradores. Es muy probable que estén incluídos en grupos privilegiados. Ud encontrará la lista de usuarios y grupos en "local users and groups" o si está en un entorno de Active Directory en "active Directory users and computers".
En ambos casos lo que debemos hacer es chequear los usuarios y los grupos tratando de identificar los NO autorizados.

3. ¿Dónde buscar el programa hackeador de modo de detenerlo?

Destaquemos que cada hack es único. Pero existen ciertos "patterns" comunes a la mayoría de los casos.

>>A. Registry Subkeys (Tipo run)

Debemos revisar en las llamadas "Registry subkeys". En particular en aquellas que hacen correr (run) programas.
Cualquier programa que Ud.no reconozca es un enemigo potencial. Si sospecha vaya a google y haga una búsqueda sobre el nombre de ese programa para ver que encuentra.
Los lugares más comunes donde están alojados estos programas son:

C:\windows y

C:\windows\system32



Las Registry Subkeys a investigar son:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

Estas llaves (validas desde Windows 9x a Windows Server 2003) instruyen a la máquina víctima a correr los programas. Vaya a: Start/run/ y ejecute regedt32.exe. En cada una de las registry subkeys antes detallada verá en el panel de la derecha los programas que se activan y donde se hallan ubicados.

Para el caso particular de NT, W2K, XP y W2003 deberá además chequear la subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\run

Las siguientes subkeys son menos comunres paro también utilizadas por los hackers:

HKEY_CLASSES_ROOT\batfile\shell\open\command
HKEY_CLASSES_ROOT\comfile\shell\open\command
HKEY_CLASSES_ROOT\exefile\shell\open\command
HKEY_CLASSES_ROOT\htafile\shell\open\command
HKEY_CLASSES_ROOT\piffile\shell\open\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\batfile\shell\open\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\comfile\shell\open\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htafila\shell\open\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\piffile\shell\open\command

Si aparece otro valor que el por "default" (por defecto) : "%1"%*, sospeche que es un programa de hackeo.

>>B. Registry subkeys de Servicios.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Las entradas debajo de estas llaves especifican los servicios de su sistema. Uno puede ver los servicios mediante una herramienta grafica. Pero tenga en cuenta que algunos servicios (llamados Type 1.) no aparecerán. Ni tampoco algunos puestos por quien nos hackea. Lo más sensato es realizar una comparación con otra máquina con el mismo SO y que estemos seguros no está comprometida.

>>C. Carpeta Startup

Haga una revision de:
C:\Documents and Settings\All Users\Start Menu\Programs\Startup
C:\Documents and Settings\user_name\Start Menu\Programs\Startup
(tenga cuidado de tener las cosas configuradas de modo que le muestre los "hidden files" también).

Chequee en:
C:\windows\tasks

>>E. Win.ini

Algunos codigos maliciosos pueden estar ocultos en: C:\windows\win.ini en la sección:
[windows]
Run=
Load=

>>F. System.ini

Es posible que un hacker use comandos de shell buscando programas en: C:\windows\system.ini
Busque en
[boot]
shell=explorer.exe<nombre del programa>

Existen otros lugares utilizados por los hackers pero estos son los más comunes.
Existe una herramienta de la empresa Sysinternals (Freeware) que nos indica qué programas se cargan al bootear nuestro sistema. (www.sysinternals.com/ntw2k/freeware/autorun.shtml). Muy recomendable (ver nota adjunta)

Es importante resaltar que es casi imposible limpiar completamente una computadora hackeada. La única forma de estar 100% seguro de que una computadora esté limpia es formatear el disco rígido y reinstalar la máquina desde cero.!!!

¿Qué son Root Kits?

Son programas silenciosos (stealth programms) que corren a nivel del SO. Abren puertos en la máquina comprometida de modo que un intruso puede hacer una conexión remota.
Conforman una colección de herramientas que permiten a un hacker crear un backdoor a un sistema. Una vez instalado coleccionar información sobre otros sistemas en la red, capturar passwords y mtrafico en la red, esconder el hecho que el sistema está comprometido, etc.

¿Qué es un backdoor ?

Un mecanismo oculto en software o hardware que puede ser activado de modo de permitir evitar mecanismos de protección a sistemas. Proveerá en general, acceso con muchos privilegios o totales al sistema ya sea con una cuenta o desde una cuenta más restringida. Es activado, de un modo de apariencia inocente. Por ejemplo, una secuencia de llaves en una terminal. Otra alternativa podría ser enviando un paquete específico a un puerto determinado. Los desarrolladores de software muchas veces introducen backdoors en sus códigos de modo de permitirles entrar en el sistema y realizar ciertas funciones (a veces se llama “mantainence hook”, gancho de mantenimiento). Los backdoors son dejados muchas veces en sistemas de producción por diseño y pero a veces por accidente. Como sinónimo se utiliza “trapdoor”.

¿Qué son Troyanos?

Un Troyano (también llamado Trojan horse, caballo de Troya) es un programa (software) en el cuál código malicioso o dañino está contenido dentro de otro progre (en apariencia inofensivo). Cuando este programa se ejecuta, el Troyano realiza una serie de acciones, normalmente realizando acciones de modo de poder persistir en el sistema víctima. Los Troyanos permiten además a los hackers a abrir “bacdoors” (puertas traseras) en nuestro sistema, dándoles acceso a los archivos y conectividad a nuestra red.



AUTORUNS una de las "SYSINTERNALS Tools"
(UN FREEWARE INDISPENSABLE EN LA SEGURIDAD WINDOWS)

Todo aquel que sea un profesional en IT conoce el nombre de Mark Russinovich. Mark es un editor y autor de la revista Windows IT Pro en US (www.windowsitpro.com) y Arquitecto de Software para la empresa "Winternals Software" Co-autor de libro "Windows internals" de Microsoft Press y de muchas utilidades como Process Explorer, Filemon y Regmon (ver www.sysinternals.com)

¿Qué es "AUTORUNS"?

"Autoruns" es una utilidad que tiene el más completo conocimiento de donde están ubicadas los programas llamados auto-start. "Autoruns", muestra qué programas están configurados para correr (run) durante el llamado boot-up del sistema (arranque) y posterior login de un usuario. Nos muestra las entradas en el orden en que Windows las procesa (en el Start-up del sistema y logon del usuario). Estos programas incluyen aquellos en la carpeta "startup", Run, RunOnce y otras Registry Keys. Uno puede configurar Autoruns de modo de que nos muestre otras locaciones, incluyendo extensiones del shell de Explorer, toolbar (barras de tareas), los llamados "browser helper objects, notificaciones Winlogon, servicios auto-start y muchos más. Autoruns supera lejos la herramienta de Microsoft MSConfig que viene instalada en Windows Me, XP y Windows Server 2003.

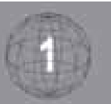
Posee una opción, "Hide Signed Microsoft Entries" (Esconda las entries firmadas por Microsoft) que nos permite concentrarnos solamente en las llamadas "auto-starting images" de terceros y que han sido agregadas a nuestro sistema posteriormente a la instalación. Tambien está incluído en el paquete que se puede descargar libremente de la web un equivalente que nos permite trabajar en línea de comandos y cuya salida está en formato CSV (autorunsc).
La figura 1 nos muestra un screenshot del display de Autoruns.Su utilización es muy sencilla y puede llevar 2 minutos aprender su uso. Una opción interesante es dehabilitar un dado programa al Stara-up con sólo destildar el correspondiente casillero. En el proximo re-start de la máquina esa aplicación no corre más en forma automática y siempre puedo volver a activarla.
Para remarcar: Autoruns nos indica el orden en que los programas son lanzados por el SO. Recordemos que los programas lanzados primero pueden ser sobre escritos por otros que comiencen a posteriori.

Si nos interesa conocer detalle del entry, en el registry de la imagen correspondiente, la empresa que la creó o el path al archivo de la imagen, podemos hacer doble clic sobre ese entry. Si hacemos boton derecho, existe la opción "google" que buscará en internet información sobre la aplicación de nuestro interés. Esto es muy útil al momento de búsqueda de un posible hack en nuestro sistema. Muy probablemente, si lo corre, se sorprenderá de cuantos ejecutables se largan automáticamente!!.
Autoruns corre en todas las versiones de Windows.
Se descarga de www.sysinternals.com.

Autoruns [COR-81\Administrator] - Sysinternals: www.sysinternals.com

File Entry View User Help

Autorun Entry	Description	Publisher	Image F
HKLM\System\CurrentControlSet\Services			
Avg7Alrt	AVG Alert Manager	(Not verified) GRISOFT, s....	c:\progra
Avg7UpdSvc	AVG Update Service	(Not verified) GRISOFT, s....	c:\progra
GEARSecurity	CD access and burning support.	(Not verified) GEAR Softw...	c:\winnt'
PAVAGENTE	Panda AdminSecure © communication service	(Not verified) Panda Softw...	c:\progra
PavAtScheduler	Panda AdminSecure Scheduler	(Not verified) Panda Softw...	c:\progra
PAVSRV	On-Access Antivirus Scanner Service.	(Not verified) Panda Softw...	c:\winnt'
VMAuthdService	Authorization and authentication service for starting a...	(Not verified) VMware, Inc.	c:\progra
VMnetDHCP	DHCP service for virtual networks	(Not verified) VMware, Inc.	c:\winnt'
VMware NAT Service	Network address translation for virtual networks	(Not verified) VMware, Inc.	c:\winnt'
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
\\Cor-comunity\EPSON Stylus C63 Series	EPSON Status Monitor 3	(Not verified) SEIKO EPS...	c:\winnt'
AVG7_CC	AVG Control Center	(Not verified) GRISOFT, s....	c:\progra
AVG7_EMC	AVG E-Mail Scanner	(Not verified) GRISOFT, s....	c:\progra
iTunesHelper	iTunesHelper Module	(Not verified) Apple Compu...	c:\progra
khooker	SiS 300/305 Super VGA Keyboard Daemon	(Not verified) Silicon Integr...	c:\progra
NeroCheck	NeroCheck	(Not verified) Ahead Softw...	c:\winnt'
PAVNT	Antivirus Tray Icon for Servers.	(Not verified) Panda Softw...	c:\winnt'
pdfMachine dispatcher			c:\progra
QuickTime Task		(Not verified) Apple Computer, Inc.	ogra
SiS Tray	SiS 300/305 Super VGA Tray Application	(Not verified) Silicon Integr...	c:\progra





Seguridad Wireless

Quizás la fuente de riesgo más significativa en una red inalámbrica sea el hecho, que el medio sostén de las comunicaciones, ondas electromagnéticas en el aire, están disponibles para los intrusos, siendo equivalente a tener puertos Ethernet

Por Leonel Becchio

Introducción

En 1999 el Standard 802.11b fue aprobado por la IEEE. Así nacen las WLANs (Wireless LANs (Local Area Networks)). Las computadoras podían interconectarse en red con un buen ancho de banda sin tener que estar conectadas por cables. Surgió la posibilidad de conectar múltiples computadoras en el hogar compartiendo una conexión a Internet común. O, juegos en red que podían realizarse sin necesidad de cables y conexiones costosas y complicadas. En la empresa la conectividad wireless y la aparición de dispositivos más reducidos permitían estar en reuniones o seminarios y aún poder estar realizando tareas como si estuviesemos sentados en nuestro escritorio. Surgió una era de "elegancia" del trabajo en red donde con una laptop y desde cualquier lugar es posible acceder a los recursos informáticos de la empresa o Intenet.
Pero que sucede con la seguridad y los riesgos de esta nueva tecnología wireless.(inalámbrica). Algunos de estos riesgos son similares a aquellos en redes por cables. Algunos están magnificados bajo una tecnología wireless. Algunos son nuevos. Quizás la fuente de riesgo más significativa en una red inalámbrica sea el hecho, que el medio sostén de las comunicaciones, ondas electromagnéticas en el aire, están disponibles para los intrusos, siendo equivalente a tener puertos Ethernet disponibles a cualquiera, en nuestra vereda.

Las comunicaciones inalámbricas son posibles gracias a las ondas electromagnéticas que pueden desplazarse a gran velocidad por el aire e incluso por el vacío. Estas ondas no son ni más ni menos que campos eléctricos y magnéticos que oscilan en cuadratura, es decir perpendiculares entre sí, a una frecuencia dada. Por frecuencia entendemos que lo hacen con cierta regularidad, una cierta cantidad de veces por segundo y siempre de la misma manera. Por ejemplo, si nos remitimos a una estación emisora de radio FM, ésta transmite a una cierta frecuencia, digamos 105.5 MHz (se lee Mega Hertz). Su antena transmite y la nuestra recibe campos electromagnéticos que oscilan a razón de ¡105,5 millones de veces en un segundo!

Este ejemplo es para que Ud. tenga una idea de lo que sucede en el aire. Pero resulta que las redes inalámbricas que comunican datos tienen asignadas bandas de frecuencias diferentes a las de la radio comercial AM y FM. Estas últimas son licenciadas y las emisoras deben pagar por su uso. Las redes inalámbricas hogareñas o empresariales tienen asignadas la banda de microondas, banda en la que operan, entre otras cosas, los hornos a microondas y algunos teléfonos inalámbricos. Esta banda es de uso libre por lo que se desarrollaron diferentes técnicas para minimizar la interferencia de las redes con otros dispositivos que operan libremente en dicha banda. Dentro de esta gama de frecuencias una muy típica es la de 2,4 GHz (Giga Hertz) cuyos campos oscilan a razón de 2.400 millones de veces por segundo en todas las direcciones.

Una red local inalámbrica o WLAN (del inglés, Wireless Local Area Network) tiene dos modos posibles de comunicación entre los dispositivos:

• ad hoc o de peer to peer (entre pares), donde un dispositivo se comunica directamente con otro de su misma especie sin la intervención de un dispositivo central (ver Figura 1).

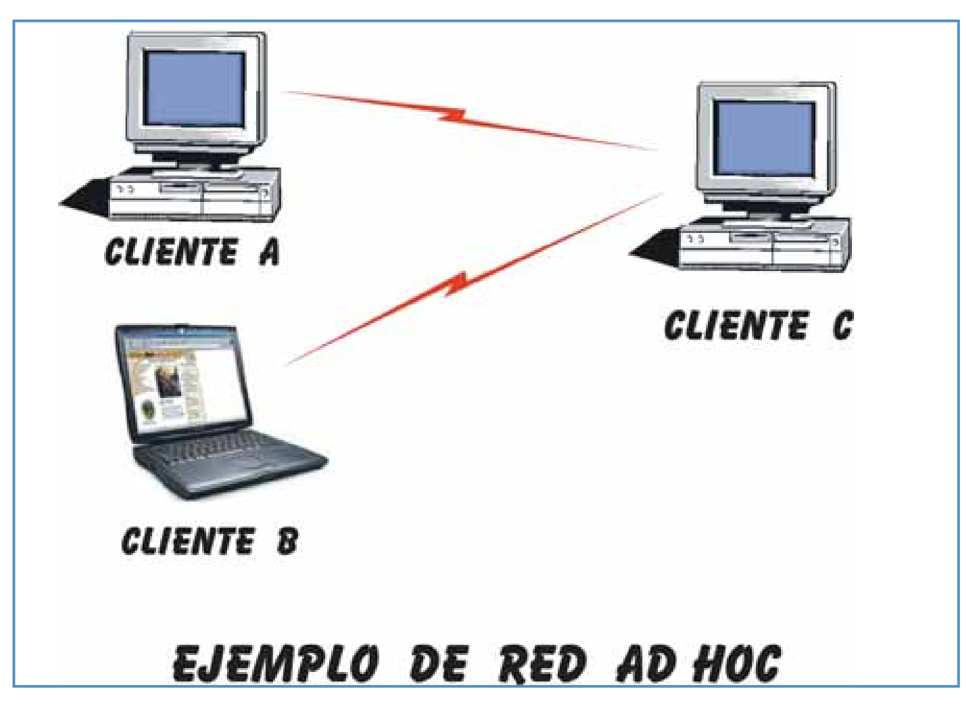


Figura 1.

• de infraestructura, donde la comunicación entre dispositivos se realiza a través de un equipo central concentrador de datos conocido como access point o punto de acceso que generalmente está conectado a una red cableada que hasta le permite acceso a Internet o una red corporativa. (ver Figura 2).

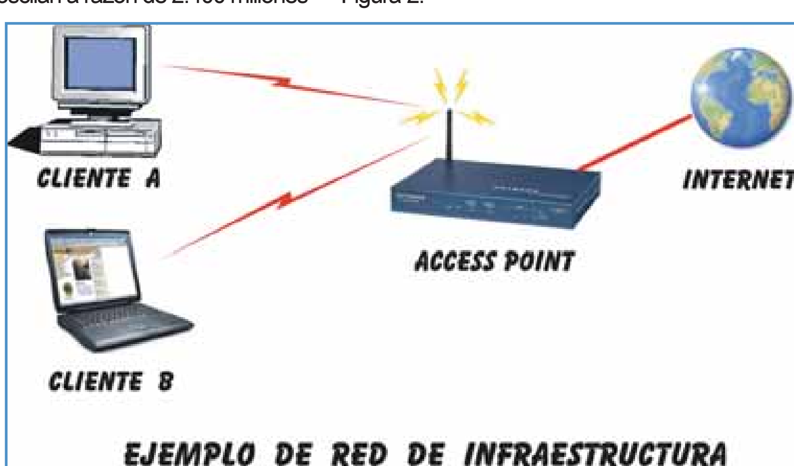


Figura 2.

Las especificaciones para el armado de una WLAN fueron establecidas en 1999 por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) bajo el estándar 802.11. Uno de los estándares utilizados hoy en día es el 802.11b que, entre tantas cosas, define una frecuencia de trabajo de 2,4 GHz, una distancia operativa que ronda los 100 metros y una tasa de transferencia de datos de 11 Mbps (mega bits por segundo). El estándar IEEE 802.11 y sus variantes a, b, g, h son conocidos como Wi-Fi por Wireless Fidelity (Fidelidad inalámbrica).
El modelo de infraestructura es el más utilizado a causa de que se implementa toda la seguridad en torno al dispositivo central o ACCESS POINT. El estándar define 15 canales que pueden ser utilizados para realizar la comunicación. Cada placa de red ubicada en cada computadora rastrea cada uno de los 15 canales en busca de una WLAN. Tan pronto como los parámetros configurados en el cliente y en ACCESS POINT coincidan, éstos iniciarán la comunicación y la computadora cliente pasará a formar parte de la red. Los canales son rastreados por la placa de red y configurados en el ACCESS POINT. Algunos modelos sólo permiten el uso de 11 canales únicamente.

Seguridad

Es muy evidente que si las ondas electromagnéticas se propagan en todas las direcciones pudiendo atravesar obstáculos como paredes, puertas y ventanas, la seguridad de nuestra empresa se verá seriamente comprometida.

Actualmente la empresa inglesa BAE Systems se encuentra desarrollando una cobertura para paredes capaz de filtrar las frecuencias que utiliza Wi-Fi dejando pasar aquellas destinadas a radio y comunicaciones celulares. El material, una suerte de capa de cobre sobre un polímero llamado Kapton, posee el mismo tratamiento que los circuitos impresos y hasta ahora era utilizado en aviones de combate. El panel tendrá un espesor de 50 a 100 micrones (milésimas de milímetro) y podrá ser aplicado a la mayoría de las superficies incluso vidrio. Aunque aún no se encuentra a la venta, la compañía asegura que no costará caro y lo comercializará a través de sus subsidiarias.

Ésta es una forma de evitar que el tráfico de nuestra empresa sea visto desde el exterior de la misma. Pero incluso existen otras técnicas que ayudan a que la información sea un poco más difícil sino imposible de ser accedida desde el exterior. Imagínese que cualquier persona podría estar interceptando información desde la calle con una simple notebook adaptada con Wi-Fi, tiempo y voluntad y estar robándole los datos de su clave bancaria mientras Ud. confía en que su sistema es ¿seguro?. A este tipo de "hacking se lo llama Wardriving.

Medidas básicas de seguridad

Existen una serie de medidas básicas a implementar para lograr una red un poco más difícil de penetrar. A pesar de que no existe una red completamente segura, lo que se trata de lograr es una red con la máxima seguridad posible.

Service Set Identifier (SSID)

Es un parámetro utilizado para diferenciar una red de otra. Inicialmente los ACCESS POINTS lo traen configurado por defecto según su marca comercial. Por ejemplo, todos los ACCESS POINTS Cisco vienen configurados como "Tsunami". El hecho de no cambiar el SSID por defecto hace que la red sea mucho más fácil de detectar. Otro error muy común es asignarle nombres significativos como el nombre de la empresa o el departamento al que pertenece el ACCESS POINT o algún nombre igualmente adivinable. El SSID debería de ser creado con las mismas reglas para la creación de PASSWORDS, es decir, poseer cierta cantidad de caracteres como mínimo, incluir caracteres alfanuméricos y simbólicos y no contener nombres fácilmente adivinables, etc.

Por defecto el ACCESS POINT difunde el SSID varias veces por segundos. La ventaja de esto es que los usuarios autorizados encuentran con facilidad la red, pero también la encuentran aquellos que no lo son. Este rasgo es lo que permite a las WLAN ser detectadas por la mayorías de los software de detección sin conocer su SSID. La forma en que los ACCESS POINTS dan a conocer el SSID es a través de la publicación al aire de información como si se tratara de una especie de faro o baliza por lo que dicha información se la conoce como tramas beacon (del inglés, baliza, faro).

Figura 3. (Configuración del SSID y el modo de comunicación en el cliente wireless)



Si de seguridad de la información se trata, habitualmente se llevan a cabo dos procesos o técnicas que, en conjunto, minimizan el riesgo de ingreso ilegal a una red. Los dos procesos son autenticación y encriptación. Autenticación se refiere al hecho de verificar la identidad del usuario para comprobar que se trata efectivamente de quién dice ser. Por encriptación se entiende que es el hecho de desmenuzar y disfrazar la información para que su lectura resulte incomprensible a aquel que no es el destinatario del mensaje.

Tipo de autenticación

Antes de que cualquier otra comunicación se lleve a cabo entre un cliente wireless y un ACCESS POINT, ellos comienzan un diálogo. Este proceso se conoce como asociación. Posterior a esto existe una etapa de autenticación donde el cliente debe acreditarse frente al ACCESS POINT y éste debe asegurarse de que aquel es quién dice ser. Esto agrega una protección extra frente al mero uso de SSID. La autenticación puede ser de dos tipos:

- autenticación abierta.
- autenticación de clave compartida.

La más simple y por defecto es la autenticación abierta donde cualquiera puede iniciar una conversación con el ACCESS POINT pues no provee seguridad alguna. Cuando se utiliza autenticación de clave compartida, el cliente le envía al ACCESS POINT una solicitud de asociación, acto seguido el ACCESS POINT le contesta enviándole una cadena de texto de desafío que el cliente debe encriptar y devolver. Si el texto fue encriptado correctamente, al cliente se le permite comunicarse con el ACCESS POINT pudiendo pasar a la próxima etapa de seguridad.

La debilidad de esta etapa reside en el envío por parte del ACCESS POINT de la cadena de texto en forma plana (sin encriptar). Si un atacante conoce la cadena de texto plano y la cadena después de haber sido encriptada, puede fácilmente conocer la clave compartida. Como veremos a continuación, WEP y la autenticación de clave compartida utilizan la misma clave para encriptar, de esta manera queda comprometida la seguridad pues un atacante podría descifrar todo el tráfico a y desde el ACCESS POINT. Irónicamente conviene configurar el modo de autenticación como abierto y dejar que cualquiera acceda al ACCESS POINT, recayendo en otros métodos que manejen la seguridad. A pesar de que remover una etapa de seguridad pueda parecer contradictorio, esta capa en particular



entorpece la seguridad más de lo que ayuda.

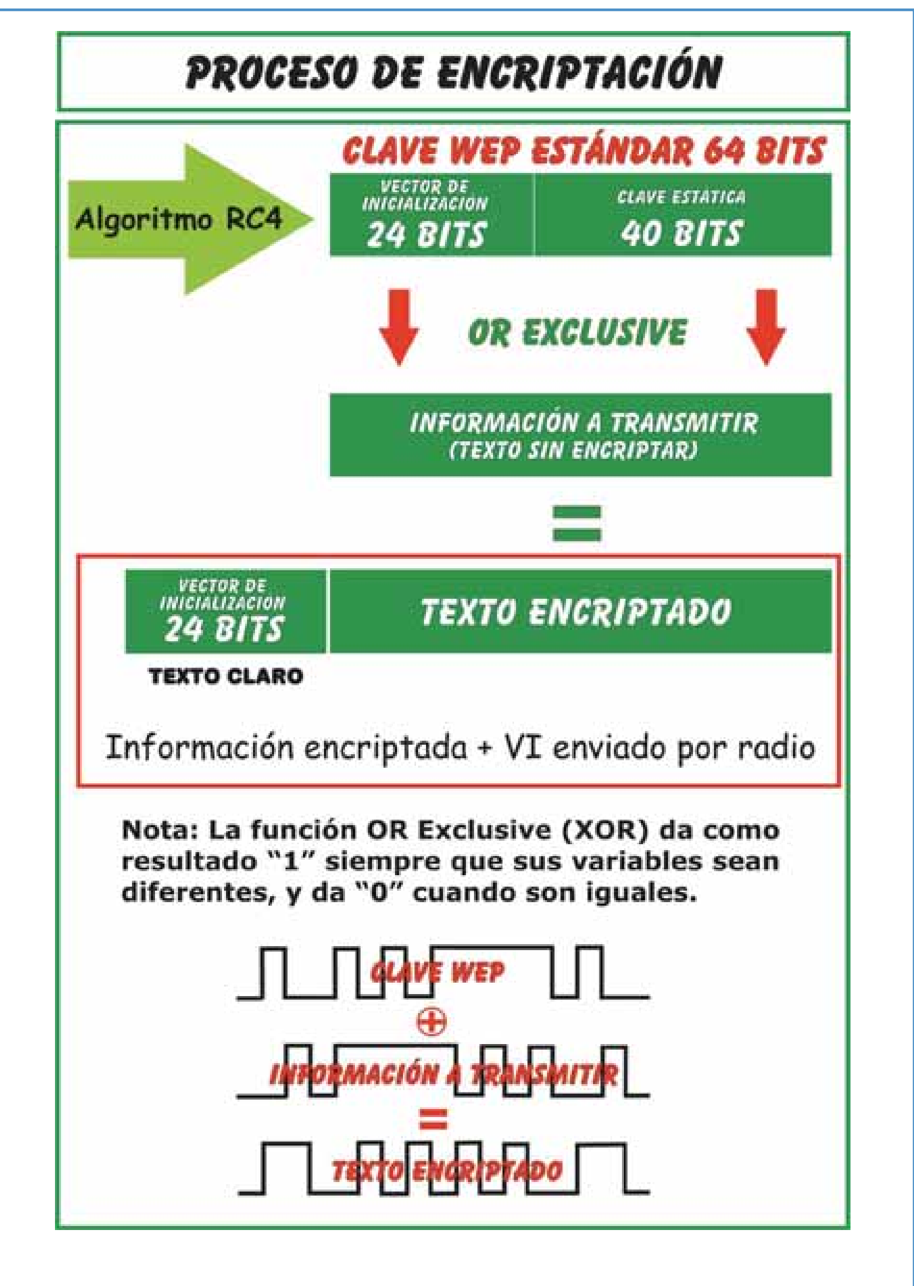
Si nos remitimos a la etapa de encriptación, existen diferentes técnicas, algunas del momento en que surgió el estándar y otras actuales.

Wired Equivalent Privacy (WEP)

WEP fue pensado para darle a una red wireless la seguridad que tienen las redes cableadas. El proceso de encriptación WEP requiere el uso de una clave estática de 40 bits introducida por el usuario.

Como dicha clave será utilizada para desencriptar el mensaje, es necesario que sea introducida en cada dispositivo de la red. Con dicha clave y un vector de inicialización (V I) de 24 bits se obtiene una nueva clave de 64 bits (40 + 24) mediante un algoritmo conocido como RC4.

La información a transmitir se la combina con esta nueva clave bajo la operación lógica OR-Exclusive (XOR) obteniéndose paquetes totalmente encriptados. A esto se le concatena el VI (en texto claro) nuevamente y se envía por ondas de radio toda esta trama. De esta manera, el dispositivo receptor recibe dicho VI y puede "mezclarlo" con su clave estática y generar la clave de 64 bits para desencriptar el mensaje. El VI es generado por el transmisor y puede cambiar con cada paquete transmitido, de modo que cada paquete nunca sea encriptado con la misma cifra.
Figura 4.



A pesar de poseer un mecanismo al parecer tan "cerrado", WEP ha sido probado como poco eficiente pues su clave RC4 es poco segura. Las razones son varias, pero explicaremos sólo algunas de ellas.

El primer ataque utiliza una vulnerabilidad detectada en la limitación numérica del vector de inicialización. A causa de sus 24 bits de longitud, se pueden armar 16.777.216 valores posibles (224). Mientras esto puede parecer mucho, tenga en cuenta que 16 millones de paquetes se transmiten en unas pocas horas en una red con mucho tráfico. Cada cierto tiempo el algoritmo genera el mismo vector de inicialización para ser reutilizado en la encriptación, por lo que mediante una escucha pasiva del tráfico encriptado se puede determinar la clave WEP dada su reiterada secuencia. Tenga en cuenta además algo muy simple: el VI viaja en texto claro (sin encriptar).

El segundo ataque se debe a la vulnerabilidad del algoritmo RC4 con ciertos vectores de inicialización conocidos como débiles. Parece ser que ciertos números entre 0 y 16.777.215 no trabajan bien en el mecanismo de encriptación RC4. Cuando se los utiliza, los paquetes mal encriptados pueden ser analizados matemáticamente por funciones que revelan parte del código WEP. Capturando una gran cantidad de éstos, un atacante puede comprometer la seguridad de la red.

Un tercer problema yace en torno a la administración de las claves. Si se decide usar WEP de acuerdo al estándar 802.11b, se debe programar la misma clave WEP en cada dispositivo cliente y ACCESS POINT. Si por alguna razón esta clave se encuentra comprometida (ya sea por empleados despedidos, porque alguien la comunicó por teléfono, o porque simplemente algún atacante pudo adivinarla) se deberá reprogramar todo nuevamente en cada dispositivo.

Esto no parece ser tan complicado si la WLAN consta de pocos dispositivos. En cambio si se trata de un campus universitario o de una gran empresa, el trabajo de cambiar las claves se convierte en una terrible pesadilla. Reiteramos además que la clave WEP es la misma clave que se utiliza para codificar el modo de autenticación por clave compartida, por lo que vulnerar ésta en la primera etapa significa que se encontrará ya vulnerada en el proceso de encriptación, no resultando conveniente la combinación clave compartida – WEP.

Figura 5. Access point. Configuración del canal de transmisión, SSID, tipo de autenticación, WEP.

Más allá de lo básico. ¿Qué hay disponible para asegurar mi red ?

Closed Network

Uno de los primeros intentos por encauzar la inseguridad de las redes inalámbricas fue desarrollado por la empresa Lucent para su equipamiento. Habían desarrollado una "red cerrada" que difería de las redes estándar 802.11b en que los ACCESS POINTS no difundían periódicamente las tramas que componen el SSID (beacon) sino cada una cantidad prefijada de tiempo mayor que en las redes estándar. A pesar de que el SSID es todavía transmitido en el aire en texto plano (sin encriptar), el hecho de retransmitirlo cada una cantidad de tiempo mayor hace que sea más difícil encontrar la red. Muchos de los clientes wireless actuales permiten el ingreso manual del SSID, medida un poco más segura que el simple proceso automático de exploración. Si bien esta técnica no resulta persuasiva frente a un ataque planificado, protege la red contra atacantes casuales.

Figura 6. Access point. Configuración del tiempo de publicación del SSID (Beacon interval).



WEP de 128 bits

La empresa Lucent también fue pionera en el desarrollo de una clave WEP de 128 bits denominada WEP Plus. Esto incrementa de 40 bits a 104 bits la clave a lo que hay que sumarle los 24 bits del vector de inicialización, resultando 128 bits totales. Esto llevaría muchísimo más tiempo determinar la clave mediante un ataque por fuerza bruta. Sin embargo todavía existen inconvenientes con el uso de 128 bits. Aunque se utilicen 128 bits (104 de clave + 24 de VI) en vez de 64 bits (40 de clave + 24 de VI), la longitud del vector de inicialización sigue siendo la misma, y ésta la causa de la vulnerabilidad. Actualmente se encuentran disponibles claves de 192 bits y de 256 bits. En la figura 4, en su parte inferior veíamos que se pueden ingresar hasta 4 claves de 26 dígitos hexadecimales (104 bits) cada una, pues se encuentra habilitado el modo WEP de 128 bits. A eso, el mecanismo de encriptación WEP le adiciona el vector de inicialización de 24 bits, resultando los 128 bits totales. Se debe especificar en cada cliente wireless, cuál de las 4 claves deberá utilizar e ingresarla manualmente.

Rotación de claves

La rotación de la clave es otro método que ayuda contra los defectos en WEP. En la especificación 802.11b existen dos claves WEP. Una es para encriptar el flujo de datos entre el ACCESS POINT y los clientes wireless, la otra es para encriptar la difusión de mensajes de broadcast tales como DHCP o peticiones ARP. A causa de que esta clave es idéntica a la clave estática WEP, la empresa Cisco introdujo la idea de que sea generada dinámicamente y que posea una vida corta. Esta característica no requiere una instalación extra pues es de muy fácil implementación. El administrador debe especificar en el ACCESS POINT una cantidad de tiempo, en segundos, y cada vez que se inicialice el contador dicho ACCESS POINT difundirá una nueva clave ¡pero encriptándola con la vieja!. Con estos parámetros no habrá el tiempo suficiente para que un atacante pueda interceptar una determinada cantidad de paquetes necesaria para corromper la clave. Este método representa sólo una parte del plan de seguridad.

Redes privadas virtuales (VPN)

Si bien las VPN han sido utilizadas desde 1990 en redes cableadas para asegurar las comunicaciones entre usuarios remotos y sus redes corporativas a través de Internet, su funcionalidad puede ser adaptada a las WLAN. Esta técnica provee una especie de túnel donde los datos viajan totalmente encriptados desde un sitio hasta el otro. Generalmente el ACCESS POINT se ubica por detrás del gateway VPN, por lo que los datos viajan encriptados aún desde la PC al ACCESS POINT.

Filtrado de direcciones MAC

Otro método a tener en cuenta es el filtrado de direcciones MAC. Toda placa de red posee un número de identificación que la hace única frente a cualquier otra placa del mundo. Éste consta de 48 bits expresados en forma hexadecimal divididos en dos grupos, 24 bits que identifican al fabricante y los 24 bits restantes que identifican al producto de dicho fabricante. A causa de que cada placa de red posee su dirección individual, se podría limitar el acceso hacia el ACCESS POINT a sólo aquellas direcciones MAC de dispositivos autorizados y bloquear el resto.

El primer inconveniente reside en la administración de direcciones. El administrador de la red debe mantener una suerte de base de datos de cada dispositivo permitido. Esta base de datos debe ser mantenida en cada ACCESS POINT individualmente o en un servidor RADIUS al que cada ACCESS POINT tenga acceso. Cada vez que se agregue o remueva un dispositivo, el administrador debe actualizar dicha base de datos. Hacer esto en una red pequeña es un trabajo poco tedioso pero hacerlo en una donde la cantidad de dispositivos ascienda a más de cien o incluso más de mil no es una solución práctica.

Sin embargo el filtrado de direcciones MAC es fácil vencerlo si se tienen las herramientas correctas. Utilizando un software de sniffing, un atacante puede monitorear el tráfico que circula por la red y fácilmente escoger del aire las direcciones MAC de usuarios autorizados y validarse como tales enviando tramas idénticas a las robadas. Reiteramos que para redes pequeñas, el filtrado de direcciones MAC se presenta como una alternativa viable mientras que para redes grandes no justifica semejante administración.

Figura 7. Access point. Configuración del filtrado de direcciones MAC.

Se puede combinar el filtrado MAC con el filtrado de direcciones IP basado en la creación de listas de acceso, especificando qué direcciones y qué puertos asociados tendrán autorización de ingreso. Incluso ciertos modelos poseen filtros de determinados sitios web. Todo esto es actualmente de fácil implementación pues los ACCESS POINT actuales poseen funciones de firewall incorporado.

Actuales técnicas de seguridad

Los problemas descriptos en lo referente a WEP han dado posibilidad al surgimiento de diversas técnicas de encriptación, algunas de finales del año 2003, con lo cual algunos equipos anteriores deberán ser reemplazados para aprovechar todos los beneficios de las nuevas técnicas. Algunos ya están preparados de fábrica y sólo será necesario una actualización de su software. WEP planteaba una única clave estática que el administrador debía cambiar, pues no lo hace por sí sola.

802.1X

(ver www.wi-fiplanet.com/tutorials /article.php /1041171)

Si bien este estándar nació para las redes cableadas, pronto fue adoptado por la industria de las WLAN y su uso se masificó. 802.1X utiliza el Protocolo de Autenticación Extensible (EAP) y un servidor RADIUS para autenticar usuarios y distribuir las claves. Esta opción es más bien empresarial y no hogareña aunque nada impide que dispongamos de un servidor RADIUS en nuestro hogar o pequeña oficina. Nota: RADIUS (Remote Authentication Dial-In User Service) es un servidor destinado a la autenticación y acreditación de usuarios que se conectan a una red. Su origen reside en los proveedores de Internet. Cuando nos conectamos a uno de ellos, debemos ingresar nuestro nombre de usuario y contraseña, el servidor contrasta dicha información con la que posee de antemano y si coinciden, lograremos conectarnos.

WEP regula el acceso a la red a través de direcciones MAC, mientras que EAP provee una infraestructura que permite a los usuarios autenticarse frente a un servidor central basado en claves públicas. El servidor le pide al ACCESS POINT una prueba de identidad la cual obtiene del usuario, acto seguido el ACCESS POINT se la envía al servidor. Cuando el servidor prueba la identidad del cliente, envía a éste y al ACCESS POINT la clave, cerrando una relación de confianza entre ambos.

Éstas técnicas aseguran también que las nuevas claves de encriptación sean generadas y distribuidas frecuentemente. Esto se conoce como distribución de "clave dinámica", un elemento esencial para obtener una buena solución de seguridad. Al expirar rápidamente el tiempo de uso de una clave, dado su constante cambio, hace que los atacantes tengan menos tiempo para recoger datos y deducir la clave. Existen actualmente una cantidad de variantes de EAP las cuales se encuentran en estudio para su probable incorporación dentro del estándar.

WPA

WPA, contracción de Wi-Fi Protected Access, es un estándar Wi-Fi diseñado para mejorar la encriptación de WEP. Fue contemplado como una solución de seguridad que no requiera de hardware adicional sino que presente como una solución actualizable vía software. Diseñado para contemplar las funcionalidades de 802.1X y EAP, pero agregándole mejoras como ser un nuevo esquema de encriptación y de distribución de claves, WPA utiliza un protocolo de integridad de clave temporal TKIP (Temporal Key Integrity Protocol) que produce una clave temporal de 128 bits para encriptar los datos.
Otros estándares como AES utilizan algoritmos matemáticos similares pero que no son completamente compatibles con los dispositivos certificados, por lo que habría que adquirir nuevo hardware. (Figuras 8 y 9) .



Figura 8. Access point. Configuración del modo WPA

Conclusiones

Si bien la seguridad al 100% no existe, todas las medidas que tomemos ayudarán a minimizar los riesgos. A continuación brindaremos una serie de consejos prácticos generales que pueden ajustarse a la mayoría de los casos.

De ser posible, debemos colocar nuestra WLAN detrás de un FIREWALL si el ACCESS POINT no incorpora funciones de tal.

Debemos escoger un SSID que no sea fácil de adivinar por el atacante, nombres largos con caracteres alfanuméricos y simbólicos alternados y, por supuesto, siempre en nuestra memoria, nunca anotado en un papelito colgado del ACCESS POINT.

Debemos habilitar WEP si no tenemos una opción de mayor seguridad como WPA.
Muchos ACCESS POINT requieren por defecto que el modo de autenticación sea por clave compartida si se habilita WEP.

Debe colocar su red en “modo cerrado”, es decir asignando un tiempo grande a la emisión del SSID por parte del ACCESS POINT.



Figura 9. Cliente. Configuración del modo WP.

Si elige WEP y su dispositivo lo permite, elija claves de la mayor cantidad de dígitos posible. Establezca filtrado MAC e IP si es posible.

Si opta por WPA, recuerde que el modo de autenticación está basado en un servidor central al que el ACCESS POINT tiene acceso (servidor RADIUS), de nada sirve filtrar direcciones MAC localmente.

Si bien hemos hecho uso de adaptadores de red y ACCESS POINTs de empresas en particular, las configuraciones pueden ser igualmente hechas en forma similar en dispositivos de otras marcas y / o modelos.







Wireless Hacking

Existen en la actualidad una serie de técnicas que derivan de una misma base y que son diferentes medios de transporte desde los cuales se intentan interceptar datos en una red inalámbrica. Generalmente las técnicas apuntan a investigar un área en busca de redes wireless.

Por Leonel Becchio

Cada vez más debe evaluarse lo crítico que puede resultar tener un sistema inalámbrico dentro de una empresa y que no se encuentre debidamente protegido. Como ya hemos visto, un descuido a la hora de configurar un access point puede poner en evidencia información sensible desde el exterior o aún interior (que es lo más terrible) de la empresa. Hemos visto una opción tal vez poco económica que constaba en cubrir una sala con un film que evitaba que las radiaciones sean captadas desde el exterior. No estamos exentos de padecer ataques ya sea por venganza, diversión u otras causas, siendo los ataques internos los que suceden en mayor medida frente a los externos, sobre todo por empleados deshonestos que, motivados por el desinterés en su trabajo, intentan atacar la empresa donde desarrollan su labor. Hoy es muy simple pues existe una gran cantidad de opciones para hacerlo. Por tal motivo debe tomar una serie de recaudos a la hora de pensar en seguridad. Debemos aclarar que las técnicas de hacking forman parte del procedimiento para realizar un test de intrusión, las que veremos a continuación son un conjunto de posibilidades para desarrollar un test de intrusión externo. No es ilegal practicarlas si el fin que se pretende alcanzar es la mera prueba de acceso para reforzar la seguridad de nuestra red. Recae en el lector la responsabilidad por todo uso diferente al explicado en el presente artículo.

Técnicas de Wireless Hacking

Existen en la actualidad una serie de técnicas que derivan de una misma base y que son diferentes medios de transporte desde los cuales se intentan interceptar datos en una red inalámbrica. Generalmente las técnicas apuntan a investigar un área en busca de redes wireless.

War Walking

El término war, guerra en inglés, fue utilizado por primera vez en la película War Games (juegos de guerra) en la cual unos jóvenes utilizaban una técnica conocida como War Calling para escanear, módem mediante, líneas telefónicas para poder atacar alguna si el módem lograba conectarlos. El término "guerra" está inspirado en ataque, aunque muchas veces solamos utilizar las técnicas de hacking para evaluar cuán segura se encuentra nuestra red de posibles ataques. La técnica de war walking consiste en recorrer a pie un área determinada en busca de un access point mal configurado que nos permita ingresar a una red en forma clandestina. Generalmente se utiliza un dispositivo manual, práctico de transportar como puede ser una PDA corriendo un software apropiado.



Figura 1. PDA – War Walking

En la foto vemos un PDA con un módulo transceiver Wi-Fi corriendo un software que indica la zona en un mapa geográfico con la ayuda de un GPS (Sistema de Posicionamiento Global) que toma referencias de un satélite geoestacionario y permite indicarlas en el mapa.

Generalmente quién realiza estos ataques tratará siempre de pasar inadvertido ya que resulta ilegal ingresar a redes privadas, además como los equipos no poseen demasiada potencia, deberán ubicarse en las cercanías de la zona en cuestión. Un equipo más sofisticado podría incluir antenas de alta ganancia acopladas a los dispositivos, incluso aquellas de fabricación casera con latas o tubos metálicos como los recipientes de papas fritas.



Figura 2. Elementos mínimos necesarios para war walking. PDA, adaptador wireless, antena casera

War Driving

Esta técnica posee la facilidad de no ir a pie sino motorizado en un automóvil equipado para tal fin. Ahora sí pueden incorporarse herramientas más complejas e incómodas de llevar a mano. Generalmente deben ir más de una persona, de modo que uno conduzca y el otro al menos opere los dispositivos y registre los eventos.



Figura 3. War Driving



Figura 4. War Driving



Formas menos disimuladas y bastante alocadas, producto del fanatismo, son las siguientes.



Figura 5 & 6. War Driving



Y una forma anticuada pero que dio origen a lo que hoy conocemos como war driving.
(Foto tomada del website de Laboratorios Bell).

Variantes de war driving pero siempre sobre ruedas son...

War Cycling

Lo mismo pero...en bicicleta.



Figura 8. War cycling

War Flying

A todo esto pongámosle alas...



Figuras 9 & 10





Figura 11. War Flying. Aquí vemos la utilización de una antena casera formada por la unión de tres latas

War Kayaking

Y hasta aquí llega la..."locura" ¿?



Figura 12. War Kayaking

War Chalking

Esta técnica consiste en detectar una red penetrable y dejar aviso para que otros puedan acceder posteriormente. Toma del inglés la palabra chalk que significa "tiza", pues los atacantes hacen uso de un trozo de tiza para indicar, mediante una simbología específica, la presencia de una red vulnerable.

Se utiliza tiza pues puede borrarse y corregirse si cambian las condiciones de la red en cuestión.

Veamos la simbología específica que se suele utilizar y ejemplos de dicha técnica.
Generalmente estos símbolos se encuentran en zonas poco transitadas como suelen ser playas de estacionamiento en cercanías de empresas. Los parámetros que suelen representarse son: el SSID de la red, si se trata de un nodo abierto o cerrado, si posee encriptación WEP y el ancho de banda.

let's warchalk..!

KEY	SYMBOL
OPEN NODE	ssid)(bandwidth
CLOSED NODE	ssid O
WEP NODE	ssid access contact (W) bandwidth

blackbeltjones.com/warchalking

Figura 13. Símbolos de War Chalking





Figura 14. War Chalking



Figura 15. War Chalking

Scanners Wireless

Hoy en día existe una vasta cantidad de herramientas utilizadas para explorar las redes inalámbricas en busca de accesos mal configurados. Existen productos comerciales o los hay gratuitos y en versiones que corren en plataforma PC o bien en una PDA para mayor portabilidad. Siempre debemos apuntar a ser más precavidos con aquellas herramientas gratuitas ya que, al tratarse de productos de consumo masivo, existe una mayor probabilidad de que seamos atacados con este tipo de software que con uno comercial.

NetStumbler & MiniStumbler
http://www.netstumbler.com

Estos scanners trabajan con redes 802.11a, 802.11b, 802.11g. NetStumbler trabaja sobre plataforma PC Windows mientras que MiniStumbler es la versión para handheld que corre Windows CE. Se define como un sniffer de redes wireless no intrusivo pues identifica a los access points que están realizando broadcast de sus nombres (SSID), además permite identificar la dirección MAC del dispositivo. Esta herramienta genera un sumario con los access points localizados con ayuda de un GPS.



Figura 16. NetStumbler

MiniStumbler 12:09

MAC	Chan	SSID	SNR
0090D100BF6C	11	WLAN	5
0090D100B93B	11	WLAN	
0090D100CC6F	11+	WLAN	10
0090D100BEC5	6	WLAN	
004033AFC3D1	10	Wireless	
0090D100CAA5	11	WLAN	17
0090D100BE02	1	WLAN	

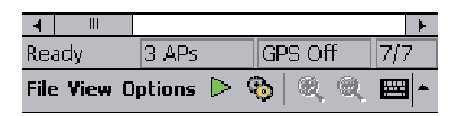


Figura 17. MiniStumbler, la versión para PDA´s

Con la ayuda de un software llamado StumbVerter, se pueden volcar los datos extraídos por NetStumbler y visualizarlos en un mapa de la ciudad a través de Microsoft MapPoint (a la fecha no se conocen mapas de Bs. As.). Los access points registrados son mostrados como pequeños conos donde sus colores y formas denotan el nivel de la señal y el modo WEP. (WiFiFofum www.wififofum.org)



Figura 18. Distribución de access points en un mapa visualizado con Microsoft MapPoint.

Básicamente se trata de un scanner 802.11 diseñado para PDA´s que corren PocketPC 2003.

Es una herramienta muy completa que no tiene nada que envidiarle a un producto comercial para plataforma PC, pues de un vistazo podemos conocer qué tipo de dispositivo es, su SSID, canal de trabajo y si tiene encripción WEP habilitada.

En su sitio web, el autor aclara que este producto NO es para uso comercial y que si se piensa usarlo con tal fin, invita a escribirle para discutir el tema de la licencia.

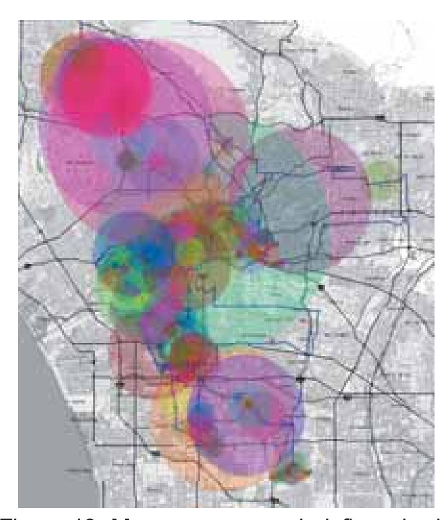


Figura 19. Mapa con zonas de influencia de acuerdo al diámetro y color de los círculos



Figura 20. WiFiFofum

AiroPeek /www.airopeek.de

Para aquellos que conocen el analizador de protocolos Ether Figura 21. WiFiFofum Peek para redes cableadas, AiroPeek es un producto con similares características pero para redes inalámbricas. Es un pro-

ducto comercial que permite “escuchar” el tráfico que circula por la red y analizarlo por protocolo.

WiFiFoFum 7:19

WEP	MAC	SSID	RSSI	Type	Cha
Off	CE:D4:42:(	glasgownet	-28	Peer	11
Off	00:60:1D:C	dcs10	-67	AP	3
Off	00:03:2F:1	MalcNet	-28	AP	1
Off	00:02:2D:2	dcs10	-43	AP	1
Off	00:02:2D:C	dcs10	-81	AP	1
Off	00:02:2D:2	dcs10	-87	AP	1
Off	00:02:2D:3	dcs10	-81	AP	1
Off	00:02:2D:2	dcs10	-87	AP	1
Off	00:30:65:1	dcs10	0	AP	1

8/9 APs GPS: Off

Tools Scan iPAQ

Figura 21. WiFiFofum

Debemos aclarar que este producto no



funciona con todas las tarjetas de red inalámbricas.

AirSnort http://airsnort.shmoo.com

Esta clase de productos cumple funciones más específicas que la mera exploración de una red.

Se define como una herramienta para redes inalámbricas capaz de recuperar llaves de encriptación.

Opera monitoreando la red en forma pasiva y reuniendo una suficiente cantidad de paquetes hasta “adivinar” la clave usada en la encriptación permitiendo especificar si se trabajará con claves de 40 ó de 128 bits.



Figura 7. Un antiguo war driver

Existe una versión de AirSnort que corre bajo Windows y otra bajo Linux.

Kismet: el sniffer wireless (inalámbrico) más popular de la lista de Fyodor. (www.insecure.org)

Fyodor, autor de nmap y quien mantiene la web page www.insecure.org realiza anualmente una compulsa sobre ¿cuáles son las herramientas más usadas por los expertos en seguridad informática?

Su mailing list recoge seguramente a los mejores expertos en seguridad informática, quienes normalmente utilizan nmap para variadas funciones.

Para el caso de un SNIFFER WIRELESS, es KISMET quién logra el lugar más destacado.

¿Qué es KISMET?
(http://www.kismetwireless.net)

Kismet es un poderoso sniffer para redes inalámbricas. Es un sniffer de red sobre el protocolo 802.11b, a y g. También es lo que se denomina un analizador de redes (network dissector). Es capaz de realizar: sniffing sobre la mayoría de las tarjetas inalámbricas, detección automática de bloques de IP via paquetes UDP, ARP y DHCP, lista de equipos Cisco vía Cisco Discovery Protocol, loggin de paquetes bajo criptografía débil y con archivos de paquetes compatibles de Ethereal y tcpdump. También incluye la habilidad de graficar las redes detectadas y rangos de redes estimados en mapas ya bajados o archivos de imágenes provistos por el usuario. El soporte para correr bajo el sistema operativo Windows está aún en desarrollo preliminar, así que en este caso Netstumbler es la opción. Usuarios Linux (y aquellos con PDAs bajo Linux) pueden querer mirar al scanner Wellenreiter.

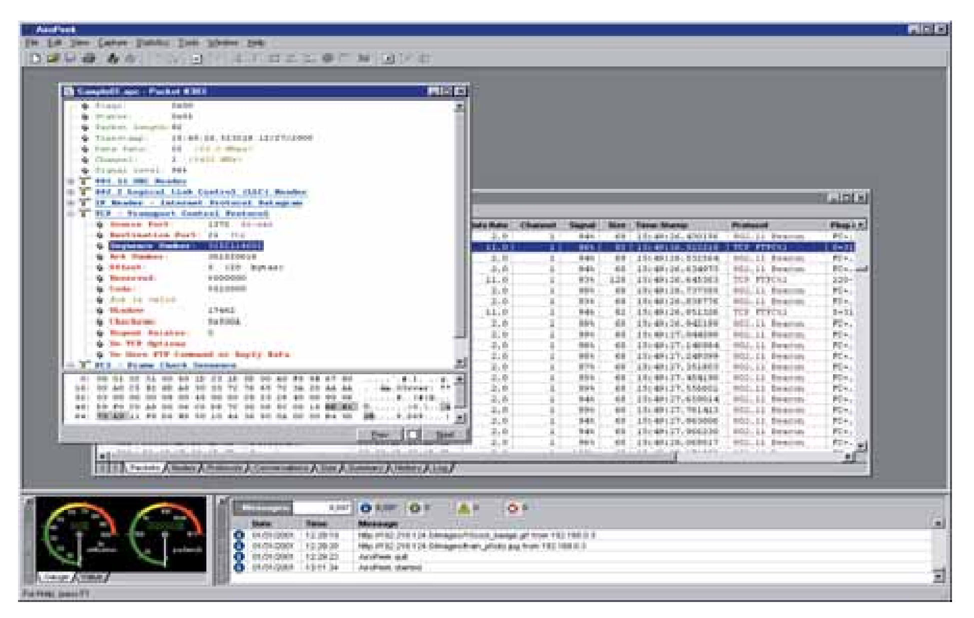


Figura 21.AiroPeek

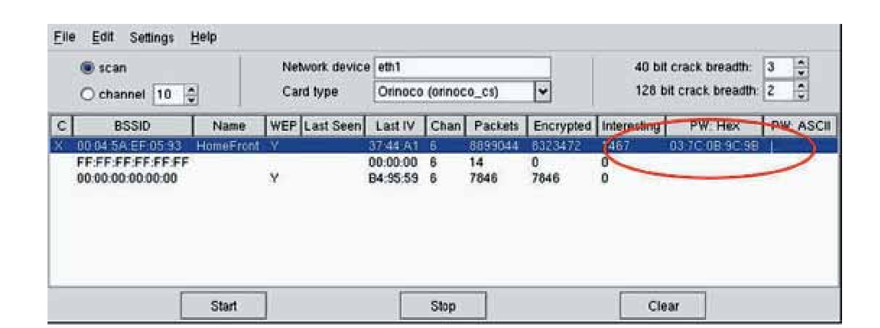


Figura 23. AirSnort ha crackeado exitosamente el protocolo WEP.

Los requerimientos para su correcto funcionamiento podrá encontrarlos en su sitio web.





802.11Seguridad

El hecho de que la información de una PC conectada a una WLAN sea accesible desde otra computadora, obliga a implementar la seguridad, para evitar que extraños puedan ver datos que no les corresponde.

Autor: David Alejandro Yanover

Director y Fundador de Master Magazine, revista digital líder en informática, con referencia en www.mastermagazine.info

Bajada

El caos que gira en torno a la protección de la redes Wi-Fi respira con la salida de una nueva especificación que busca satisfacer a los sectores más exigentes. Recorremos las soluciones actuales hasta llegar a WEP2.

Desarrollo

La disponibilidad de zonas Wi-Fi en la sociedad creció de manera notable en estos últimos años, teniendo su mayor expresión en Estados Unidos, impactando en Europa y llegando lentamente a Latinoamérica. Básicamente, ya sea una PC, notebook, teléfono móvil u otro dispositivo con soporte Wi-Fi, que se encuentra con una LAN inalámbrica (WLAN), tiene acceso a Internet. De esta manera, resulta cada día más habitual encontrar puntos de conexión o Hotspots en aeropuertos, restaurantes y comercios, siendo una forma de atraer al público. Sin embargo, es precisamente la facilidad de acceso a las redes WLAN uno de sus mayores desafíos, en el ámbito de la seguridad. Es uno de los aspectos más débiles, inclusive en entornos corporativos, donde, en varios casos, la implementación de estas tecnologías está a la espera de mejoras técnicas en el área, que garanticen la confiabilidad del tráfico de datos. Por otro lado, es extraordinario ver cómo redes privadas de empresas no aplican medidas para proteger la información. La salida de la norma 802.11i tiene previsto cambiar las cosas.
El hecho de que la información de una PC conectada a una WLAN sea accesible desde otra computadora, obliga a que sean analizadas las opciones de seguridad, para evitar que extraños puedan ver datos que no les corresponde. Es importante destacar que los puntos de conexión son fáciles de detectar, ya que revelan su presencia estando en actividad.

Una medida falsa de seguridad

Nos proponemos entonces hacer un análisis de las distintas medidas de protección que abundan hoy en el mercado. Al iniciar el camino nos topamos con WEP (Wired Equivalent Privacy). Presentado como el primer estándar de seguridad, se trata de una opción que jamás logró obtener la confianza de los técnicos a raíz de que sus sistemas invitan a los intrusos. Haciendo uso de claves compartidas, cada usuario de la red necesita tener su equipo configurado con la contraseña asignada para entrar en la WLAN. Durante las conexiones, WEP reserva 24 bits para resolver claves que varían con el tiempo de manera automática y se constituyen con las originales, sin embargo el procesamiento de estos datos no utiliza ninguna herramienta de codificación. No obstante, pueden hacerse algunos agregados a WEP, para establecer un mayor reto a los que tratan de invadir la red. Para monitorear las PCs que participan en la WLAN pueden usarse listas de control de acceso basadas en direcciones MAC (Media Access Control).

Herramientas de intrusión

Los sistemas que utilizan la seguridad WEP son fáciles de romper, lo cual queda reflejado en dos aplicaciones especializadas, AirSnort y Kismet. Ambos programas son capaces de resolver de manera pasiva las claves que son ejecutadas en las WLAN bajo WEP, aprovechando sus debilidades de encriptación. Al quebrar la red, es posible hacerse pasar como usuario legítimo, y observar y modificar los datos del resto de los miembros de la conexión. Por otro lado, una vez destruido WEP, las filtraciones MAC de los usuarios, en caso de utilizarse, son visibles.

Sin embargo, es aconsejable activar WEP antes que no establecer ningún parámetro de seguridad. Otro punto que interviene en la inseguridad de los puntos de conexión inalámbricos son los ataques de negación de servicios (DoS, Denial of Service). De esta forma, la capacidad de radio puede afectarse, transfiriéndose datos a un ritmo superior de que la red es capaz de soportar.

La transición: en búsqueda una solución

Luego, destaca en la lista WPA (Wi-Fi Protected Access), una de las soluciones más usadas hasta la fecha, ya que emplea métodos de encriptación de 128 bits y autentificación EAP (Extensible Authentication Protocol), además de operar con sesiones dinámicas. Lanzado en noviembre de 2002 por la Alianza Wi-Fi, encargada de certificar las normas de conectividad inalámbricas, WPA tenía como objetivo reemplazar a WEP y servir de estándar provisional, hasta que hiciera su aparición IEEE (Institute for Electrical and Electronics Engineers) 802.11i.

Temporal Key Integrity Protocol (TKIP) es otra propuesta de seguridad a partir de WPA, la cual emplea claves de sesión dinámicas de 128 bits. Mientras WEP usa claves estáticas, TKIP envía una contraseña maestra a los usuarios autentificados de la WLAN al mismo tiempo que funciona de parámetro de partida para generar claves auxiliares.

Otras tecnologías de seguridad que sugiere el organismo Wi-Fi son servidores RADIUS, para trabajar con claves de acceso en usuarios inalámbricos y remotos, VPN (Virtual Private Network), que supone un canal más seguro entre el usuario y la red, Firewalls, para controlar los datos salientes y entrantes de las máquinas de tal manera de impedir que usuarios sin autorización tengan acceso a la información, y Kerberos, servicio de autentificación desarrollado en el MIT (Massachussets Institute of Technology).

El lanzamiento de una norma real de seguridad.

Cuando la seguridad en las redes wireless estaba en su peor momento, habiendo decepcionado a los entornos corporativos e inmersa en duras críticas, es presentado, en septiembre 2004, WPA2, dos meses después de la ratificación del estándar 802.11i sobre el cual está basado. WPA2 proporciona la administración segura de las conexiones Wi-Fi, garantizando un completo monitoreo de los usuarios activos. Entre las características principales destacan el uso de métodos de encriptación AES y el hecho de ser compatible con WPA, su antecesor, por lo que es posible migrar a esta nueva especificación.

Las WLAN comienzan a consolidarse, respondiendo a las necesidades de los ámbitos más exigentes. La aparición de WPA2 es uno de los mayores logros en el campo de la seguridad. Aún es temprano para decir que todos los problemas de intrusión desaparecerán, pero la implementación de las medidas que se han puntualizado debería ser suficiente para que las redes trabajen sin preocupaciones.



NMap y las 75 mejores herramientas de seguridad.

No existe página más prestigiosa que insecure.org. En ella, Fyodor desarrolla NMAP, la herramienta Número 1, y presenta las 75 mejores herramientas de seguridad.

Por Carlos Vaughn O'Connor

NMAP ("Network Mapper") es una herramienta Open Source, para exploración de redes y auditoría de seguridad. Se diseñó para scanear rápidamente redes de gran escala, aunque funciona muy bien aplicada a hosts individuales. Usa los paquetes IP de manera novedosa para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y su versión) ofrecen esos hosts, qué sistemas operativos (y sus versiones) están empleando, qué tipo de filtros/firewalls están en uso, y muchas características más. Nmap puede correrse en la mayoría de las arquitecturas y se puede emplear tanto en versiones de consola como gráficas. NMAP es software libre, disponible con todo su código bajo la licencia GNU/GPL.

Si desea aprender cómo funciona nmap como herramientas de scanning, lea el artículo "Ethical Hacking Paso a Paso. Scanning" en esta revista.

Características de Nmap:

-**Flexible**: Dispone de docenas de técnicas avanzadas para lo que se denomina scaneo de redes ("mapping out networks") llenas de filtros IP, firewalls, routers y otros obstáculos. Esto incluye muchos mecanismos de escaneo de puertos (TCP y UDP), detección de sistemas operativos, detección de versiones, barrido de ping (ping sweeps) y más.

-**Poderoso**: Ha sido usado para el scaneo de redes inmensas con cientos o miles de máquinas.

-**Portable**: Corre en la mayoría de los sistemas operativos, incluyendo Linux, Windows de Microsoft, FreeBSD, Open BSD, Solaris, Irix, Mac OS X, HP UX, NetBSD, Sun, Amiga y otros.

-**Fácil**: Ofrece características avanzadas para usuarios avanzados A la vez usted puede comenzar con tan simplemente hacer "nmap -v -A hostblanco". Existen versiones para línea de comandos y GUI de modo de satisfacer cada preferencia. Existen los binarios para aquellos que no deseen compilar a Nmap desde las fuentes.

-**Sin cargo**: El objetivo primario del Proyecto de Nmap es hacer Internet más seguro y proveer a Administradores/auditores/hackers de una herramienta avanzada para explorar sus redes. Nmap está disponible para ser bajado gratuitamente (free download), pero también viene con el código fuente completo que Usted puede modificar y redistribuirlo bajo los términos de GNU General Public License (GPL).

-**Bien documentado**: Fácil de comprender y actualizada documentación que usted podrá encontrar en www.insecure.org, en múltiples lenguajes.

-**Con Soporte**: No tiene garantía, pero su autor puede ser consultado (fyodor@insecure.org) Existen muchas listas de correo a las cuales usted podría pertenecer.

-**Aclamado**: Ha recibido numerosas distinciones de revistas e incluso Microsoft la recomienda. Recibió el "Information Security Product of the Year" de la revista Linux Journal, Info Works y CodeTalker Digest.

-**Popular**: Miles de personas la bajan diariamente y está incluida en muchos sistemas operativos (Red Hat, Debian Linux, Gentoo, FreBSD, OpenBSD, etc). Está entre los primeros diez (de 30.000) programas que se ofrecen en Freshmeat.net. Esto es importante ya que le brinda a Nmap un desarrollo vibrante y lo soportan activamente.

Encuesta a 20.000 usuarios de Nmap: las 75 mejores herramientas de seguridad informática.

De una encuesta realizada por Fyodor a 20.000 hackers que utilizan Nmap, con el propósito de que describieran sus herramientas de seguridad favoritas, respondieron 1854 personas. Cada persona podía responder con una lista de 8 herramientas.

Aquí detallaremos las 5 primeras herramientas y mencionaremos las 6 siguientes. Quien desee ver la lista completa lo referimos a www.insecure.org.
Los interesados en el tema de seguridad encontrarán información de utilidad en la



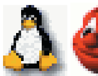
lista y podrán también conocer productos con los que todavía no están familiarizados. Dada la característica especial de los consultados, las respuestas tendrán una leve orientación hacia los ataques más que a la defensa.

 *Hay que pagar*

 *Trabaja bajo Linux*

 *Trabaja bajo FreeBSD /NetBSD /OpenBSD y UNIX propietarios*

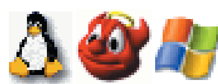
 *Trabaja bajo Windows*

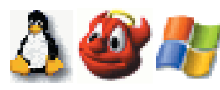
1-Nessus: Es la herramienta más importante, Open Source, de testeo de vulnerabilidades.
Es un scanner de seguridad remoto para Linux, BSD, Solaris y otros Unix. Está basado en plug-ins, tiene una interfase GTK y lleva a cabo 1200 chequeos de seguridad remotos. Permite que los reportes sean generados en HTLM, XML, LaTex y texto ASCII y sugiere soluciones para problemas de seguridad.

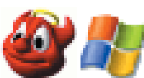
2-Ethereal: Sniffea los paquetes TCP/IP que mantienen unida a Internet.
Es un analizador de protocolos de red de softaware libre y corre bajo Unix y Windows. Le permite examinar los datos de una red en actividad o de un archivo del disco que contenga el material capturado. Usted puede interactivamente browsear los datos capturados, viendo un resumen y la información detallada de cada paquete. Tiene varias características poderosas., incluyendo una exposición rica y filtrada y la habilidad de ver el stream reconstruido de una sesión TCP. Está incluida, una versión en modo texto llamada Tethereal.



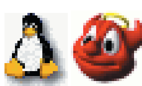
3-Snort: Un sistema de detección de intrusos (IDS) de software libre.
Es liviano, capaz de realizar análisis de tráfico en tiempo real y registro de los paquetes IP de las redes.
Puede realizar análisis de protocolo, búsqueda / correspondencia de contenidos y puede ser usado para detectar una variedad de ataques y pruebas, como buffer overflows, stealth port scans (scans de puertos en modo silencioso), ataques CGI, pruebas SMB, intentos de caracterizaciones de sistemas operativos y mucho más. Usa un lenguaje basado en reglas flexibles para describir el tránsito que debe recolectar o pasar y un dispositivo de detección modular. Mucha gente aconseja que la herramienta " Analysis Console for Intrsion Databases (ACID)" sea usado en conjunto con Snort.



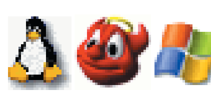
4-Netcat. Se trata de la "navaja del ejército suizo" (Swiss army knife).
Es una herramienta Unix que lee y escribe datos a través de las conexiones de red, usando protocolos TCP o UDP. Se diseñó para ser una herramienta confiable back-end que puede ser usada directamente o fácilmente transportada por otros programas y scripts.
Al mismo tiempo es una herramienta con muchas características para hacer un debugging y explorar, ya que puede crear casi cualquier tipo de conexión que usted puede necesitar y tiene varias capacidades incluidas.

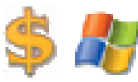
5-TCP Dump / Win Dump: El clásico sniffer para monitorear la red y adquirir datos.
Es un analizador de paquetes de red (sniffer) muy conocido y apreciado. Puede ser usado para printear los headers (encabezamientos) de los paquetes en una interfase de red que coincidan con una dada expresión. Se puede usar esta herramienta para hallar problemas de redes y para monitorear las actividades de las mismas. Hay una portación llamada WinDump para Windows. TCPDump es también la fuente del Libpcap/WinPcap, la librería de captura de paquetes usada por Nmap. Note que muchos usuarios prefieren el sniffer Ethereal que es más nuevo.



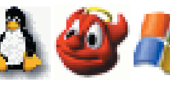
6-Hping2 : Una utilidad para sensar las redes. Es un ping en esteroides.



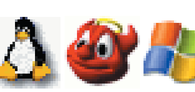
7-DSniff: Un grupo de herramientas poderosas para auditar redes y realizar tests de penetración.



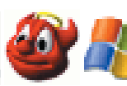
8-GFI LAN guard: Un scanner de seguridad comercial para Windows.



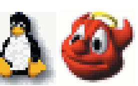
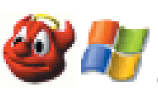
9-Ettercap: En caso de que usted todavía crea que LANs switcheadas le aportan mucha más seguridad, conozca esta herramienta.



10-Wisker /Libwisker: un scanner que permite testear servidores http, en particular vulnerabilidades CGI.

11-John the Ripper: Es un cracker de hashes de passwords multiplataforma, extraordinariamente poderoso, flexible y rápido.

12-OpenSSH/ SHH: una manera segura de acceder a computadoras remotas.



13-Sam Spade: Herramienta freeware para Windows, que nos permite indagar en la redes.

¿Quién es Fyodor?

Se trata de un hacker (definido por él "...como quien se divierte jugando con las computadoras y empujando al hardware y software a sus límites"...), que tiene interés en la seguridad, las redes y la criptografía. Estos temas se superponen pero son esenciales para la seguridad de las redes públicas como es Internet.
Su actividad favorita es programar y aún sabiendo muchos lenguajes, la mayoría de su trabajo lo hace en C/C++ o Perl. Se siente cómodo en máquinas corriendo bajo UNIX, especialmente en sistemas open source. Su opinión es que estas plataformas son muy poderosas, pueden redistribuirse llibremente y vienen con una colección muy grande de software de utilidad. La disponibilidad del código fuente los hace más seguros y más fáciles de utilizar y comprender. Su scanner de seguridad Nmap ahora corre bajo Windows y por ello se ha esforzado en aprender lo básico de ese ambiente de programación.
Como muchos hackers, le gusta leer. Se inspiró en el autor ruso Fyodor Dostoyewski para su elegir su "handle" (seudónimo).


USERS
ARGENTINA $6,90
(RECARGO POR ENVIO AL INTERIOR $0,20)
#08
.code
COMUNIDAD DE DESARROLLADORES
BANG!
Guerra en la Web
PHP / ASP.NET / JSP / COLDFUSION
Varias tecnologías quieren imponer su reinado. Investigamos a fondo todas las opciones y preparamos una comparativa como sólo .code puede hacerlo.
¿Cuál es mejor para cada tipo de desarrollo?
C# Programación de sockets en .NET para establecer comunicaciones entre aplicaciones | Themes y Skins, nuevas características de estilos en ASP.NET 2.0
PHP Aplicaciones de escritorio para Windows con PHP y la librería GTK | Review: Component One Studio | Toolbox: Trucos para Visual FoxPro | Software factory .code
MANAGEMENT Administración exitosa de proyectos: tiempos, costos y recursos | Entrevista: Renato Quedas, Senior Software Architect de Borland Latin America
ADEMAS Guía de recursos: programas y componentes para charts | Noticias | Recomendaciones de software y libros | Opiniones | Correo de lectores
WHITE PAPER: METODOLOGIAS AGILES
9 789875 262492
cod
08

SNORT bajo Windows

EL NIDS (Network Intrusion Detection System) OPEN SOURCE ahora corriendo bajo Windows.

Introducción

Infinidad de paquetes con información atraviesan a gran velocidad las redes de computadoras.
Algunos fueron diseñados con malas intenciones. Pueden pasar los firewalls y las defensas perimetrales ingresando y dañando nuestros sistemas.

Seguramente, ha experimentado algún ataque con SQL SLAMMER, CODE RED, NIMDA y MSBlaster. Todos estos programas maliciosos utilizan protocolos confiables: HTTP o SMB/CIFS de Microsoft para alcanzar a realizar su maligna función.

La opción NO es bloquear esos protocolos. Las organizaciones emplean los llamados IDS (Intrution Detection Systems) (Sistemas de detección de intrusos). En particular, aquellos que monitorean las redes: los NIDS (Network IDS).

Es posible encontrar en el mercado excelentes NIDS. Sus precios y capacidades son variados. Generalizando son todos buenos y cumplen su función con eficacia.

Existe además una versión de fuente abierta (Open Source) denominada SNORT.
A diferencia de lo que ocurre generalmente esta aplicación Open Source del mundo Unix-like (Linux, OpenBSD…) corre en Sistemas Operativos de Microsoft. Y se trata de un producto muy eficaz.

La historia de SNORT

SNORT fue desarrollado alrededor de 1998 por Martin Roesch (el fundador de Sourcefire, http://www.sourcefire.com /snort.html) y ofertado con licencia GPL/GNU .Se trata de un aplicación ampliamente probada, realizada con contribuciones de la comunidad Open Source. La versión actual puede llevar a cabo en tiempo real un análisis del tráfico IP y su registración (loggin) aún en redes con Fast Ethernet y Gigabit Ethernet . Snort fue mirado a la plataforma Windows (Win32) por Michael Davis. Chris Reid ha continuado esta tarea y actualmente SNORT para Windows está presentado como un ejecutable de muy sencilla implementación.

¿Se necesitan muchos recursos para correr SNORT bajo WINDOWS?

>> SNORT corre bajo SOs Windows desde WIN2k professional y posteriores (XP, Win2K Server, Windows Server 2003).
>> Se necesita por lo menos una placa de red. Quizás la mejor opción es tener 2 placas de red. Una conectada a la red a monitorear y otra a nuestra red de producción.
>> No se requiere licencia ya que es una aplicación OpenSource.
>> No son necesarios demasiados recursos computacionales. El programa es muy eficiente. Por ejemplo SNORT con 900 MHz y 512MB de Memoria puede manejar redes de miles de sistemas.

¿Dónde ubico un NIDS dentro de mi infraestructura de red?

Muy probablemente no lo colocaré delante del firewall. La idea es dejar al firewall filtrar. Si lo pongo delante obtendré la mayor cantidad de paquetes, pero también de ruido.
También deberá estar detrás de los dispositivos que reciban a sus usuarios remotos (VPNs, conexiones wireless…).
Recordemos que si el tráfico está encriptado SNORT no lo detectará. Como regla general Ud debería colocar el NIDs tan atrás como le permitan los componentes que encriptan el tráfico, pero debe poder capturar el tráfico de tantos segmentos y subredes como sea posible.

¿Cómo instalo SNORT en un Sistema Operativo Windows?

Snort es básicamente un sniffer de redes seteado en modo promiscuo. En el mundo Unix se utiliza “libpcap” como el driver para captura de paquetes. Loris Degioanni hizo la portación (“to port”, migrar) para Windows en el producto “ WinPcap”.
¿Entonces qué es winPcap?. Es un filtro de paquetes que opera a nivel del kernel, es una DLL de bajo nivel y una librería de alto nivel (independiente del sistema): wpcap.dll (basada en libpcap 0.6.2) .
Se puede bajar WinPcap en http://winpcap.polito.it. Winpcap también soporta el excelente sniffer del mundo oPen source: “Ethereal” (www. ethereal.com). Instalar WinPcap es muy sencillo.

Snort puede obtenerse de la página web de Codecraft.
CodeCraft ha sido responsable por
>> Escritura y mantenimiento del Win32. Ha realizado la migración de Snort1.8,1.9,2.0 y 2.1 de Unix,
>> soporte inicial para Microsoft SQL. Servidor en el módulo loggin de la base de datos.
>> Desarrollar el soporte integrado para Snort para correr como un servicio Win32.
>> Desarrollar la instalación de Snort wizard paraWindows.

http://www.codecraftconsultants.com/Snort .aspx o www.snort.org

Una vez realizado el download de la página de Codecraft, la instalación es más que sencilla. Deberá tomar algunas decisiones en el camino como por ejemplo, qué base de datos utilizará: MySQL o ODBC (en este caso deje la selección por default). Pero, quizás quiera hacerlo a una base SQL o Oracle. El resto son simple decisiones de ubicación de archivos, etc.

Aquel que desee usar Snort de forma profesional podrá usar la documentación de su web-page o excelentes libros dedicados a Snort. Allí aprenderá a:
-Configurarlo.
-Configurar las reglas.
-Setear las alertas y los logs.
-Correrlo como un servicio.

Pero, veamos cómo funciona Snort.

Al momento de ejecutar el .exe la siguiente información deberá ser provista: 1. dónde escribir los logs y 2. dónde encontrar el archivo de configuración.

Esta información se provee cuando lanzamos snort desde la línea de comando:

snort –l C:\snort\log –c C:\etc\snort.conf –A console

-A le dice que deberá mostrar la salida en la pantalla.

La figura 1 nos muestra la salida de snort a esta secuencia de comando en el command prompt. A partir de este momento Snort analizará todo lo que ocurre en su red.

Si desea activar una alerta intere- 




```
C:\>snort -l c:\snort\log -c\snort\etc\snort.conf -A console
Running in IDS mode
Log directory = c:\snort\log
Initializing Network Interface \Device\Packet_NdisWanIp
OpenPcap() device \Device\Packet_NdisWanIp network lookup:
        The operation completed successfully.
        --== Initializing Snort ==--
Initializing Output Plugins!
Decoding Ethernet on interface \Device\Packet_NdisWanIp
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file \snort\etc\snort.conf

++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
,-----------[Flow Config]----------------------
| Stats Interval:   0
| Hash Method:      2
...
      IIS Unicode Map: GLOBAL IIS UNICODE MAP CONFIG
      Non-RFC Compliant Characters: NONE
rpc_decode arguments:
    Ports to decode RPC on: 111 32771
    alert_fragments: INACTIVE
    alert_large_fragments: ACTIVE
```

sante, simule lo que hace el ataque de Nimda y Code Red:
Desde su web.browser haga:
http://www.prueba.com.ar/cmd.exe (prueba es por supuesto genérico).

Verá en la otra pantalla la alerta que nos da Snort y por supuesto también quedará grabado en c:\snort.log
Se recomienda tener cuidado con el sitio web que se usa ya que muchos administradores considerarían esto como el ataque de un hacker.
Otro modo de activar de forma sencilla un alerta es enviar un ping a un servidor de nuestra subred con un paquete extremadamente grande :

ping -l 32767 192.168.0.33

este paquete dirigido a la máquina con número IP 192.168.0.33, no es de rutina y Snort nos dará la alerta.

Más allá del primer nivel.

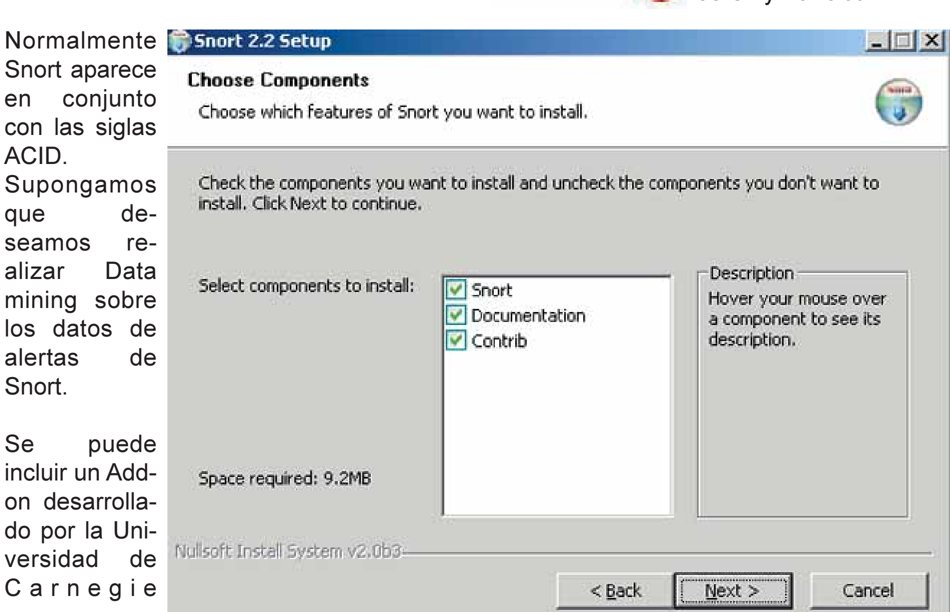
Lo anterior fue "jugar" a ver como funciona Snort. Snort es una aplicación muy completa. Y, es posible incrementar sus posibilidades. Recomendamos leer la bibliografía sobre Snort para volverse un experto. En nota aparte les mostramos un libro muy popular sobre como utilizar Snort.

¿Qué es ACID?

Normalmente Snort aparece en conjunto con las siglas ACID. Supongamos que deseamos realizar Data mining sobre los datos de alertas de Snort.

Se puede incluir un Add-on desarrollado por la Universidad de Carnegie Mellon que permite realizar esto (ACID: Análisis Console for Intrusión Databases.

¡¡Una herramienta casi indispensable!

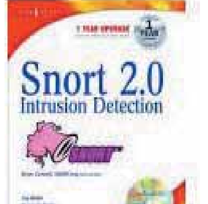


¿Qué es un NIDS?

NIDS es básicamente un SNIFFER especializado. Un "olfateador" de paquetes. Estudia cada paquete que pasa por la interfase tratando de localizar determimadas formas precisas dentro del payload de los paquetes donde residen específicamente los códigos maliciosos.

Con un NIDS como SNORT podrá vigilar dentro de su red, el contenido y la correspondencia de cada paquete que atraviesa su organización y detectar así una gran cantidad de ataques y tráfico hostil.

¡Todo esto en tiempo real!



Snort 2.0 Intrusion Detection

por Brian Caswell,
Jay Beale,
James C. Foster,
Jeremy Faircloth.

SNORT, el sistema de detección de intrusos de la fuente libre

"SNORT es un sistema de detección de intrusos de tipo liviano. Es capaz de llevar a cabo en tiempos reales un análisis del tráfico y logonear un paquete en trabajos de red IP.
Está preparado para hacer análisis protocolizado, buscar contenidos y unirlos y puede detectar variedad de ataques y pruebas como neutralizar sobreflujo, escanea rport steath, ataques CGI, pruebas SMB, intentos de huella digital y mucho más."

"Snort usa un lenguaje de reglas flexibles para describir el tráfico que debe recolectar o pasar, así como una maquinaria de detección que utiliza una arquitectura modular de conexión. Snort también tiene capacidad de alerta de tiempo real., incorporando mecanismos de alerta para syslog, un archivo específico de usuario, una conexión UNIX, o mensajes de Winpop a los clientes Windows utilizando el smbclient de Samba."

"Tiene 3 usos primarios. Puede ser usado directamente como un sniffer de paquetes similar a tcpdump (1), un logger de paquetes (de utilidad para el trabajo de red de tráfico debugging, etc.) o como detector de intrusión en el sistema."

-Extractado de snort.org

Snort para Linux

autor: Martin Sturm
MCSA, MCSE, LPIC (101/102/201)

¿Qué es Snort?

El Snort es un Sistema de detección de Instrusos (IDS) muy potente, el cual hace las veces de sniffer colocando la interfaz de red de la máquina en la cual se encuentra corriendo en modo promiscuo, es decir, brinda la capacidad a la placa de red de obtener todos los paquetes que circulan en un mismo hub o switch aún sin ser los suyos.

El objetivo de Snort es, por sobre todas las cosas, el de alertar en caso de recibir un intento de ingreso o ataque a nuestra red. Para ello se basa en un gran número de reglas que deciden si el evento o paquete recibido corresponde a un ataque o no.

Una de las ventajas más importantes a la hora de optar por Snort como nuestro IDS preferido por sobre los demás, es la gran cantidad de reglas que se encuentran predefinidas hoy en día y el respetable grupo de desarrolladores con el que la organización cuenta, ya que estos últimos son quienes constantemente actualizan dichas reglas. Una regla se encuentra definida por dos secciones lógicas: Cabecera de la Regla ó **"Rule Header"** y Opciónes de la Regla ó **"Rule Options"** donde:

Cabecera de la Regla: Contiene la acción, protocolo, puerto e IP/máscara de red Origen y puerto e IP/máscara de red Destino.

Opciónes de la Regla: Contiene mensajes de alerta e información del sector del paquete donde se debe inspeccionar para determinar si esta se cumple o no.

En el siguiente ejemplo se generará un alerta en caso que alguien intentara conectarse al servidor Telnet local, el mismo arrojará un mensaje con el valor especificado en "msg", lo que permitirá identificar rápidamente el evento en el archivo de log:

alert tcp any any -> 192.168.1.1/32 23 (content: "pass"; msg: "TELNET!!!!";)



Es muy importante prestar gran atención a la configuración del mismo, ya que si éste se encuentra configurado con una sintaxis errónea podría generar lo que se conoce como "Falsos positivos", es decir, estaría informando alertas falsas, las cuales no harán más que llenar el disco de información innecesaria.

¿Cómo instalarlo?

Para instalar Snort se deberá bajar el código compreso de su sitio oficial (www.snort.org); en la sección "downloads" se encuentran las versiones disponibles, las mismas pueden bajarse precompiladas (en formato binario) o bien para compilar. Una vez obtenida la versión que más se ajuste a las necesidades se procederá a la instalación:
En caso de haber optado por el paquete rpm:

```
rpm –Uvh snort-1.9a.rpm
```

Este procedimiento es muy sencillo, ya que al instalar el paquete rpm, automáticamente se crean los directorios con las diferentes reglas y el archivo de configuración principal del programa.

En caso de haber optado por el source:

```
$ tar zxf snort-2.0.0.tar.gz
$ cd /snort-2.0.0
$ ./configure
$ make
$ make install
```

Una vez instalado el source se deberá instalar el paquete de reglas actualizadas, el cual incluye el archivo de configuración general, este mismo puede ser obtenido también dentro de la sección "downloads" de la página oficial (www.snort.org).

```
$ mkdir /etc/snort
$ cp snortrules-stable.tar.gz /etc/snort
$ tar -zxfv snortrules-stable.tar.gz
$ rm snortrules-stable.tar.gz
```

Luego se procederá a la edición del archivo de configuración principal mediante cualquier editor de texto:

```
$ vi /etc/snort/snort.conf
```

Al editarlo se podrá observar gran cantidad de líneas comentadas, las mismas ayudarán a la comprensión de cada una de las opciones a configurar. Las opciones más importantes para configurar son las siguientes:

Definición del rango de direc-



ciones de la red interna:

Para ello se deberá optar por alguna de las posibilidades descriptas (sólo una)

var HOME_NET 192.168.0.0/24
Define un rango de direcciones de red.

var HOME_NET $eth0_ADDRESS
Define el rango de direcciones de red al cual pertenece la interface de red eth0 al iniciar Snort

var HOME_NET [192.168.0.0/24 ,192.168.1.0 / 24,10.0.0.0/24]
Define diversos rangos de direcciones de red.

Definición del rango de direcciones de la red externa:

var EXTERNAL_NET any

Definición de direcciones de red de algunos servidores importantes:

var DNS_SERVERS [192.168.0.1, 232.0.17,24.132.21.0.18]

var SMTP_SERVERS 192.168.0.1

var HTTP_SERVERS [192.168.0.2, 192.168.1.2]

var SQL_SERVERS [192.168.0.1]

Una vez configuradas las variables más importantes se deberán habilitar los diversos preprocesadores, los cuales se encargarán de analizar los paquetes y detectar intentos de hackeo, ataques, escaneo de puertos, y demás.

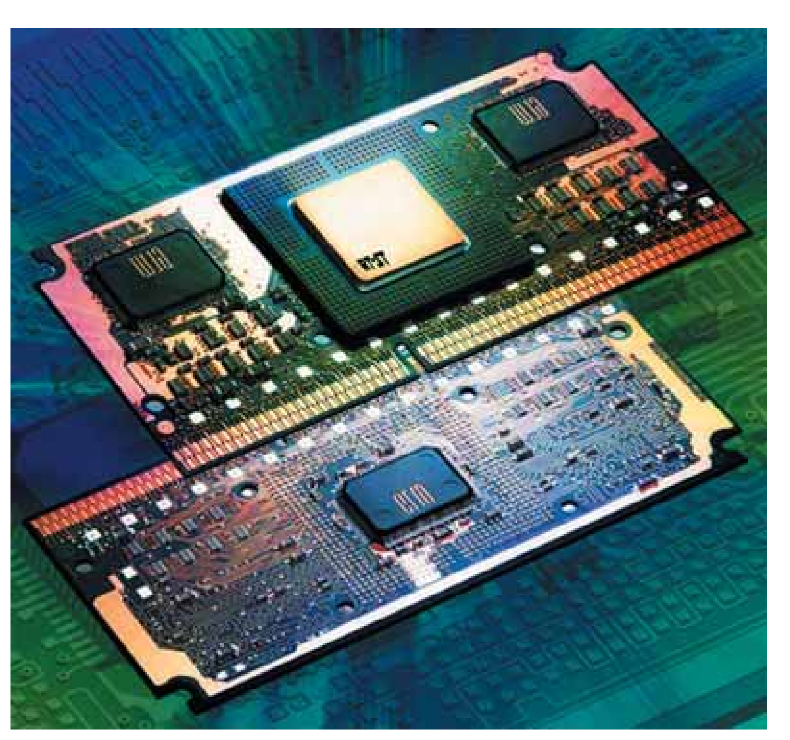
El mecanismo a seguir para la activación de los diferentes preprocesadores es la de visualizar los comentarios de cada una de las opciones para reconocer cuáles son los que se ajustarán a las necesidades y luego descomentar cada una de las líneas, por ejemplo, para activar la detección de escaneo de puertos se deberá activar el procesador "portscan", para ello habrá que descomentar la siguiente línea:

**preprocessor portscan:
192.168.1.0/24 5 7
/var/log/portscan.log**

La sintaxis afirma que si en 7 segundos se accedieran a 5 puertos distintos, entonces la información quedará reflejada en el archivo de log "portscan.log".

**preprocessor portscan-ignore-hosts:
192.168.1.1/32 192.168.0.1/32**

En este caso se estaría ignorando cualquier tipo de scaneo de puertos proveniente de los hosts especificados.



Finalmente, se deberán configurar las salidas (Output) de información, es decir, qué tipos de registros generar (utilizando Syslog, archivos de textos propios, registros en una base de datos), dónde se alojarán dichas salidas y cuál será su formato.

En caso de necesitar reflejar los eventos en el syslog se deberá descomentar la siguiente línea donde se podrá apreciar tanto la facilidad como el argumento del syslog:

**output alert_syslog:
LOG_AUTH LOG_ALERT**

Si por el contrario se deseara arrojar la información de los eventos a una base de datos (MySQL) se deberá descomentar la siguiente línea:

**output database:
log, mysql, user=snort
password=ppp
dbname=snort host=localhost**

Cabe aclarar que en caso de arrojar la información a una base de datos, previamente se deberán instalar los paquetes necesarios para el funcionamiento del Servidor SQL (Mysql / Postgresql).

Además al momento de compilar el snort se deberá parametrizar el soporte para SQL:

./configure --with-mysql

La información recolectada por el Servidor de base de datos puede ser consultada por línea de comandos o vía web mediante un soft adicional llamado ACID, quien se encargará de la visualización de los logs recogidos por Snort, este soft no necesita ningún tipo de instalación, simplemente se deberá bajar el paquete tar.gz del sitio http://acidlab.sourceforge.net/, descompactar el archivo en algún directorio dentro del "DocumentRoot" (por ejemplo /acid) correspondiente a la configuración del Servidor apache y luego acceder a la interfaz web vía: http://direccion-del-virtualhost/acid/acid_main.php

En la sección final del archivo de configuración se invocan todas las reglas incluídas dentro del directorio /etc/snort, las mismas contienen definiciones de alertas como la comentada en el ejemplo del comienzo.

Para incluir nuevas reglas tan solo hay que agregar una línea al final del archivo con el siguiente formato:

include $RULE_PATH/regla _nueva.rules



NESSUS

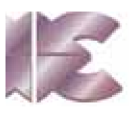
El scanner de vulnerabilidades Open Source.

La redes modernas deben ser monitoreadas de modo de poder detectar vulnerabilidades en los sistemas que las componen. Si no lo hace nuestro administrador, lo hará un hacker.

Un scanner de vulnerabilidades se aplica sobre un dado sistema y la información que obtiene se chequea (compara) contra una base de datos de vulnerabilidades conocidas. Al final nos provee un reporte de los agujeros de seguridad (security holes) encontrados.

Existen scanners de vulnerabilidades comerciales cuyos costos pueden estar en los miles de dólares. Nessus es de la misma calidad que la mayoría de ellos pero su costo es cero (gratis) y su código Open-Source.

En un reciente artículo de la prestigiosa revista WindowsITPro (www.windowsitpro.com) se realizó una comparación entre NESSUS y otros scanners de vulnerabilidades comerciales. NESSUS comparó muy favorablemente con Retina de e-eye, que fue elegido como el más destacado. Otros a destacar: Sunbelt Network Security Inspector (SNSI) de la empresa Sunbelt, Vulnerability Manager de NetIQ, LANguard Network Security Scanner de GFI, Retina de e-eye Digital Security y RMS vulnerabibity-management solution de BindView. Destacamos, que LANguard figura como número #8 en la lista (Nessus es el primero) de los más populares en la lista de Fyodor (www.insecure.org) (ver el artículo en esta edición).



Los scanners mantienen bases de datos que categorizan y describen las vulnerabilidades que pueden detectar.

Los más completos hasta proveen la posible solución a la vulnerabilidad detectada o links a las listas de Bugtraq (www.securityfocus.com) (ver nota) y CVE (Common Vulnerability and Exposures) (http://www.cve.mitre.org)(ver nota).

La mayoría de los scanners requieren tengamos que tener privilegios de administrador sobre la máquina estudiada. Aunque se provee casi siempre la opción de hacer el estudio sin ese privilegio, es decir como atacante anónimo.

Al finalizar el scaneo se produce mucha información que es presentada como un reporte. La mayoría provee archivos .mdb. Muchos para un SQL server. Si uno conoce de base de datos puede procesar la información en otros formatos.
Conocida la vulnerabilidad es también importante conocer la solución. La mayoría nos provee de suficiente información para hacerlo o aún ya nos da el remedio.

NESSUS

Nessus está compuesto de 2 partes: un cliente y un servidor. Se necesita un sistema UNIX-like como server (Linux por ejemplo). El cliente Nessus puede instalarse en una máquina bajo Windows o Unix-like (Unix, Linux, FreeBSD…).

Por ejemplo, su puesta en marcha sobre un sistema Linux es muy sencillo.

Configuración del server UNIX por el administrador

1. hacer un download e instalar nessusd(servidor) y nessus (cliente).

2. crear una cuenta en el servidor nessusd. El servidor nessusd tiene su propia base de datos de usuarios, pudiendo tener cada usuario su propio conjunto de restricciones. Esto nos permite compartir un solo server nessusd en un red amplia y restrigir a diferentes administradores a poder testear sólo su parte de la red.

La utilidad nessus-adduser me permite crear nuevas cuentas. Puedo por ejemplo, a través de reglas, permitir a un usuario sólo poder testear a un sólo host. Incluso sólo su host.

3. configurar el demonio nessus.
En el archivo /usr/local/etc/nessus /nessusd.conf se pueden setear opciones varias. Típicamente los recursos que le permitiremos usar a nessusd, la velocidad en la que debe leer los datos, etc.

4. activar "nessusd"
Una vez que esto está hecho, puedo activar "nessusd" como usuario "root" haciendo:

```
nessus -D
```

Usar el cliente UNIX o Windows:

La interfase gráfica y sus diferentes solapas me permitirán decidir qué deseo hacer . La figura 1 muestra la GUI para el caso de un cliente UNIX.

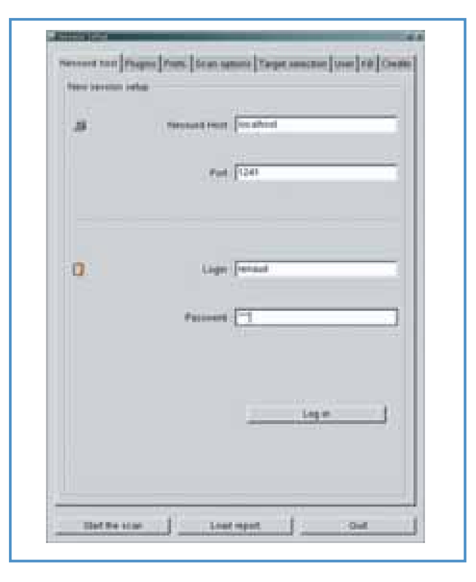


figura 1.Interfase gráfica del cliente Nessus bajo LINUX

Como ya dijimos, Nessus cliente también se puede instalar sobre plataforma Windows. Uno puede hacer un download en http://nessuswx.nessus.org.

Recalquemos que siempre se debe instalar un back-end server sobre Unix. El cliente (front-end) puede correr sobre UNIX o Windows. Usar un cliente Windows puede traer problemas de credenciales que se deberá resolver. Existe excelente documentación en los sitios detallados anteriormente donde se podrá consultar.

Nessus provee una muy completa base de datos para el chequeo de vulnerabilidades. Son llamados plugins. Es posible (si así se desea, operar a Nesus en un modo intrusivo) (ver nota).

En la página web de Nessus es posible obtener más de 2100 plugins que cubren la mayoría de las plataformas. Los plugins se organizan por familias: abusos CGI, firewalls, ftps, scanners de puertos etc…

Lo primero que hacemos al realizar un scan es crear una "session" donde definimos el blanco y opciones (hostname, o número IP o podemos importar una lista

de blancos de un archivo txt.)

Nessus incluye Network Mapper (nmap) de Fyodor (www.insecure.org). Pero, da la posiblidad de realizar otros tipos de scanning de puertos (ping,o SNMP por ejemplo).
Desde la interfase gráfica uno elige los plugins que usará. La figura 2 nos muestra la GUI donde elegimos los plugins deseados para el caso de un cliente Windows. Los plugins se pueden habilitar por familia o individualmente. Como ya referimos, es posible pedir no usar plugins intrusivos (botón: “Enable Non-DoS”(habilite No-Denial of Service, negación de Servicio).



NESSUS lanza el “Manage Session Result” (un resumen ordenado de los resultados para cada máquina estudiada) (figura 3 y 4).

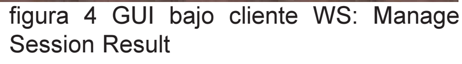


figura 4 GUI bajo cliente WS: Manage Session Result

figura 2 GUI del cliente Nessus mostrando la elección de plugins

El resultado del scan aparece en otra ventana. Allí se puede ver el progreso en tiempo real. Las vulnerabilidades encontradas son clasificadas como Holes, Warnings, Infos y Ports (agujeros, Alertas, Infos y Puertos).

Cada vulnerabilidad hallada se clasifica por su peligrosidad: high, médium o low (alta, media o baja). Terminado el Scan, uno puede exportar la salida a archivos HTML, PDF o TXT. Tambien es posible exportar para MySQL o archivo propietario.

En la info provista aparece una descripción de los problemas hallados. La salida no es muy sofisticada y aparece como una larga lista.a estudiar.

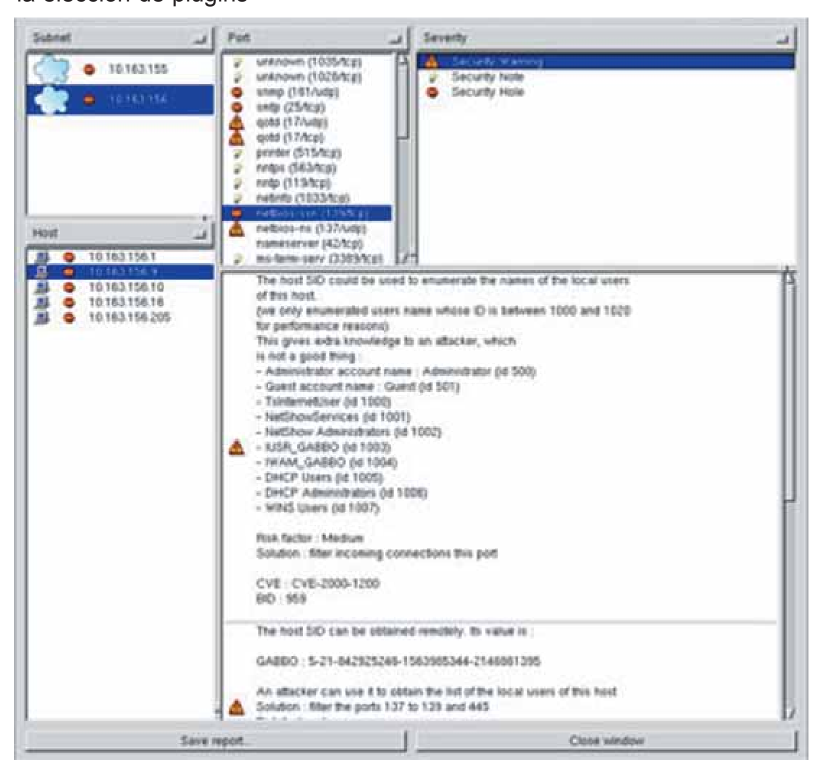


figura 3. Cliente Linux de Nessus con un report.

NESSUS y Tenable Network Security (Historia y negocio)

Nessus es el scanner de vulnerabilidades open-source más popular del mundo. Y, es usado mundialmente por cerca de 75.000 organizaciones que le permiten auditar dispositivos y aplicaciones “críticos” a un costo cero.

El proyecto Nessus fue comenzado por Renaud Deraison en 1998 con la idea de proveer a la comunidad de Intenet un scanner remoto de seguridad gratis, poderoso, actualizado y de muy sencillo uso. Está ubicado actualmente entre los productos más prestigiosos de la industria de seguridad y avalado por organizaciones muy prestigiosas tales como el SANS Institute (www.sans.org).

En el año 2002, Renaud co-fundó Tenable Network Security (www.tenablesecurity.com) conjuntamente con Ron Gula, creador de Dragon Intrution Detection System y Jack Huffard. Esta empresa es la única desarrolladora y licenciadora del código Nessus, la marca “Nessus” y del dominio nessus.org. Está ubicada en Columbia, MD, USA.
Tenable ofrece productos de software focalizados en 3 áreas de la seguridad de la información: >>Decubrimiento de vulnerabilidades y Administración
>>Administración de Eventos de seguridad
>>Comunicación Técnica y Ejecutiva





Scanning Intrusivo

Se denomina así cuando la herramienta usada trata de realizar un "exploit" de la vulnerabilidad encontrada en la máquina que estudia. Diferentes herramientas usan distintos niveles de intrusión. Debemos tener mucho cuidado al realizar estos tests de no ejecutar (por error) un exploit sobre un sistema en producción.



Common Vulnerabilities and Exposures (CVE®) es:

Una lista de nombre estandarizados de vulnerabilidades y otra información sobre "exposures" de seguridad. CVE pretende estandarizar los nombres de todas las vulnerabilidades y debilidades de seguridad conocidas públicamente.

>> CVE es un diccionario, NO una Base de Datos

>> CVE es un esfuerzo COMUNITARIO

>> Está abierto a ser revisado o bajado (downloaded).

Nota: CVE considera que el término "vulnerabilidad" tiene diferentes usos. Por tanto es importante hacer una distinción cuando es necesario. Se introdujo el término "security exposure" de modo de poder referirse a hechos de seguridad que justamente NO conforman dentro de "vulnerabilidad" para todo el mundo. Por ejemplo, este modo más restrigido de entender al término vulnerabilidad hace que por ejemplo se ponga a "finger" como una "exposure".

¿Qué es BugTraq?

(extractado de las FAQ de www.securityfocus.com)
BugTraq es un "maling list" (lista de personas suscriptas para recibir e-mails) de exposición completa y moderada, para la discusión "detallada" y anuncios de vulnerabilidades en la seguridad de computadoras: qué son, cómo abusar de ellas ("exploit") y cómo solucionarlas.

¿Cuál sería un contenido apropiado?

Uno deberá seguir los siguientes lineamientos sobre qué tipo de información deberá ser posteada en la lista de Bugtraq:

>>Información sobre vulnerabilidades en seguridad de computadoras y redes (UNIX, Windows NT y otros)
>>Programas de "exploit" (abuso), scripts o procesos detallados referidos al punto anterior
>>Patches (parches), "workarounds"(como encontrarle la vuelta) y "fixes" (arreglos).
>> Anuncios, consejos o avisos.
>> Ideas, planes futuros o trabajo en progreso relacionados con seguridad en redes/computadoras.
>> Material de información relativo a contactos en vendors (fabricantes) y procedimientos.
>> Consejos de incidentes o reportes informativos.
>> Herramientas de seguridad nuevas o mejoradas.

¿Qué contenido es inapropiado?

>> Propaganda de productos
>> Preguntas básicas ("how to´s")
>> Material de seguridad que nada tiene que ver con redes/computadoras.
>> Información sobre otro nuevo troyano o virus, a menos que sea muy especial.

¿La lista se encuentra moderada?
Sí y es Dave Ahmad <da@securityfocus.com> el moderador.
Breve Historia

¿Cuándo se creó BugTraq?

BugTraq fue creada en Noviembre 5, 1993 por Scott Chasin. Aleph One tomó mando el martes 14 de Mayo de 1996. Sobre los años, se ha transformado en una lista de seguridad muy respeta con más de 27.000 suscriptores.

¿Cómo fue que se hizo moderada?

Esto sucedió el 5 de Junio de 1995. Al mismo tiempo se la movió a netscape.org. Se hizo moderada cuando el nivel de ruido se volvió inaceptable.

¿Cómo me suscribo?

Enviar un e-mail a bugtraq-subscribe@securityfocus.com. El contenido del tema o cuerpo del mensaje no tienen importancia. Ud. Recibirá un email, respuesta, que deberá contestar.

Linux, con la lupa en la seguridad.

Fuente: www.hispasec.com

A continuación vamos a enumerar una lista de distribuciones Linux que ponen énfasis en las herramientas para aumentar los niveles de seguridad. Es importante aclarar que todas funcionan como “Live CD” lo que quiere decir que se ejecutan directamente desde el CD, no hace falta instalarlas. Esto es particularmente útil en los casos en que lo que necesitamos es una herramienta para revivir el disco o recuperar los datos.

Como varias de las distribuciones que presentamos a continuación están basadas en Knoppix, comentaremos que esta distribución es un CD arrancable con una colección de programas GNU/Linux software, detección automática de hardware, y soporte de muchas tarjetas gráficas, tarjetas de sonido, dispositivos SCSI y USB y otros periféricos. KNOPPIX puede ser usuado como una demo de Linux, CD educacional, sistema de rescate, o adaptado y usado como plataforma comercial de demos de productos. Como ya hemos dicho NO es necesario instalar nada en el disco duro. Debido a la descompresión en demanda el CD tiene casi 2 GB de programas ejecutables instalados en él.



Knoppix STD 0.1b

STD (Security Tools Distribution) es una versión personalizada de Knoppix. Utiliza el núcleo 2.4.20 y KDE 3.1, da soporte a una gran cantidad de dispositivos de hardware (que son detectados y configurados automáticamente). Cuando se arranca la máquina con Knoppix STD, no se realiza ningún tipo de modificación en la configuración de la computadora.

Todas las herramientas de Knoppix, al igual que toda la distribución, están diseñadas para ser ejecutadas directamente desde el CD y están divididas en varias categorías: herramientas para la gestión de redes; herramientas para la realización de valoraciones de seguridad y herramientas para la realización de pruebas de redes; un gran número de herramientas para la realización de pruebas de penetración, sniffers; herramientas para el análisis forense, cortafuegos, honeypots, sistemas de detección de intrusiones ; autenticación, identificación de contraseñas y cifrado.

LocalAreaSecurity 0.4

Muy pequeña (185 MB), pensada para instalarse en un CD chico, como los tipo tarjeta de crédito. También está basada en Knoppix y utiliza el núcleo 2.4.20.
LocalAreaSecurity está pensado para la realización de pruebas de verificación de la seguridad y pruebas de penetración. Para eso cuenta con un gran número de herramientas especializadas: sniffers, cifrado, monitoreo de redes, detección de información oculta, obtención de información, etc.

Phlak (Profesional Hacker's Linux Assault Kit) 0.1

Basado en Morphix. Viene con dos GUI livianas (fluxbox y XFCE4). Está especializada en la realización de análisis de seguridad, pruebas de penetración, análisis forense y auditorios de seguridad.
Incluye herramientas de análisis de tráfico, de protocolos, de funcionamiento del sistema, de extracción de datos de sistemas de archivos, cifrado de archivos, sniffers, etc.

R.I.P. (Recovery Is Possible)

Esta distribución, está pensada para recuperar datos de sistemas de archivos dañados. Funciona con lso sistemas de archivos ext2, ext3, reiser, jfs, xfs, ufs, NTFS, FAT16 y FAT32.

WARLINUX 0.5

Es una distribución live CD pensada específicamente para identificar las redes inalámbricas que están al alcance y realizar auditorías y verificaciones de los niveles de seguridad de las mismas.

F.I.R.E.



Esta versión de Linux incluye las herramientas necesarias para la realización de valoraciones de seguridad, respuesta a incidentes de seguridad, pruebas de penetración y análisis forense de sistemas y recuperación de datos en sistemas Windows, Solaris (SPARC) y Linux (x86). Adicionalmente, FERIO incluye un programa para la detección de virus (F-Prot).
Existen otras distribuciones similares a estas: Penguin, Sleuth Kit, @stake Pocket Security Toolkit v3.0, ThePacketMaster, Linux Security Server y Trinux.

Más Información:

Knoppix-STD
http://www.knoppix-std.org/

LocalAreaSecurity Linux
http://www.localareasecurity.com/

PHLAX
http://www.phlak.org/

RIP Linux
http://www.tux.org/pub/people /kent-robotti/looplinux/rip/

WARLINUX
http://sourceforge.net/projects/warlinux/

FIRE
http://biatchux.dmzs.com/

Penguin Sleuth Kit
http://www.linux-forensics.com /downloads.html

@stake Pocket Security Toolkit v3.0
http://www.atstake.com/research/tools /pst/

ThePacketMaster Linux Security Server
http://freshmeat.net/projects /tpmsecurityserver/

Trinux
http://trinux.sourceforge.net/

Lo anterior evidencia que existe una enorme cantidad de herramientas puestas a nuestra disposición.

Lo más interesante de esto es que podemos contar con sistemas operativos completamente funcionales sin necesidad de instalarlos, esto es muy útil, cuando NO PODEMOS instalarlos justamente debido a que nuestro sistema ha dejado de responder.

Aunque debemos destacar que la existencia de estas herramientas no nos absuelve de la responsabilidad de realizar backups de nuestros datos ni de prestar la debida atención a las configuraciones de seguridad de nuestras redes; el dicho es muy viejo pero sigue siendo cierto y muy aplicable a las Tecnologías de la Información: “mejor prevenir que curar”.



Microsoft



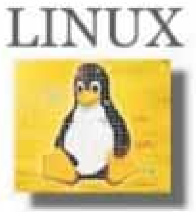
Security



WEB Design



LINUX



Suplemento Guía Cursos y Carreras - 1 Agosto 2004 a 31 Julio 2005



www.cortech.com.ar

Garantía de Educación



Un alumno, cuando "compra" un curso no busca otra cosa más que ADQUIRIR UN APRENDIZAJE, capacitarse, aprender, y crecer en el mundo de IT conociendo siempre las últimas tecnologías. La Garantía de aprendizaje COR, permite a TODOS los alumnos re-cursar cuantas veces sea necesario las Carreras o Cursos de COR TECH.

Aprovechá la posibilidad de volver a hacer tus cursos; ya sea si te quedaste con dudas, o faltaste alguna que otra clase, o simplemente porque deseas conocer el perfil de otro profesor o volver hacer el curso para conocer gente nueva.

En COR no comprás UN CURSO; comprás UN APRENDIZAJE (y queremos asegurarnos de dártelo).

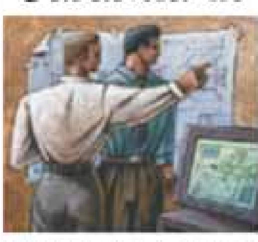
Garantía de Precio



COR Technologies garantiza ofrecerte un precio 10 % más bajo para cualquier presupuesto de Educación o consultoría en Buenos Aires o en el Interior del País. Presentando el presupuesto de la competencia (ya sea por escrito o por e-mail; para un mínimo de 2 Alumnos ó mínimo de $1000) COR te brinda la Capacitación o la Solución buscada a un costo 10 % mas bajo (sólo multiplicá tu presupuesto por 0,90 y obtené el precio que te ofrece COR).

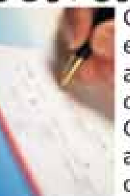
La Garantía de precio será respetada siempre y cuando el precio cobrado finalmente no sea menor al costo de realizar la Capacitación / Consultoría. COR Technologies se reserva el derecho de validación de los presupuestos propiamente presentados.

Garantía de Consultoría



Una característica de nuestras consultorías es que COR garantiza la completa conformidad de Cliente; o se reintegra el monto total de lo abonado para la misma. La Garantía de Consultoría permite al cliente estar confiado de que recibirá lo que desea; y que COR garantiza el resultado del problema mediante la Solución oportunamente propuesta.

COR Cheks



COR premia la Capacitación entregándole a todos nuestros alumnos la suma correspondiente de CORCheks. Cada CORChek es equivalente a un Peso; para ser utilizado en cualquiera de nuestros Cursos y Carreras. Los CORCheks no son transferibles; y no pueden utilizarse junto a otras promociones.

Microsoft Certified Systems Administrator (MCSA) Windows 2003

Microsoft CERTIFIED Technical Education Center — Microsoft CERTIFIED Partner for Learning Solutions

EXAMEN - Client	CURSO - Client
Examen 70–270: Installing, Configuring, and Administering Microsoft Windows XP Professional	**Curso 2285:** Installing, Configuring, and Administering Microsoft Windows XP Professional (Duración **16 hs**)
EXAMEN - Networking	**CURSO - Networking**
Examen 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	**Curso 2273:** Managing and Maintaining a Microsoft Windows Server 2003 Environment (Duración **40 hs**)
Examen 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2276:** Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts (Duración **16 hs**)
	Curso 2277: Implementing, Managing, and Maintaining a MS Windows Server 2003 Network Infrastructure: Network Services (Duración **40 hs**)
EXAMEN - Elective	**CURSO - Elective**
Examen 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**)
# Cursos: 5 (cinco) **MOC's incluidos: 5 (cinco)**	**Duración Total: 136 hs**



Microsoft Certified Systems Administrator (MCSA Sec.) Security on Windows 2003 // Track Recomendado //

EXAMEN - Client	CURSO - Client
Examen 70–270: Installing, Configuring, and Administering Microsoft Windows XP Professional	**Curso 2285:** Installing, Configuring, and Administering Microsoft Windows XP Professional (Duración **16 hs**)
EXAMEN - Networking	**CURSO - Networking**
Examen 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	**Curso 2273:** Managing and Maintaining a Microsoft Windows Server 2003 Environment (Duración **40 hs**)
Examen 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2276:** Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts (Duración **16 hs**)
	Curso 2277: Implementing, Managing, and Maintaining a MS Windows Server 2003 Network Infrastructure: Network Services (Duración **40 hs**)
EXAMEN - Elective	**CURSO - Elective**
Examen 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**)
Examen 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network	**Curso 2823:** Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración **40 hs**)
# Cursos: 6 (seis) **MOC's incluidos: 6 (seis)**	**Duración Total: 176 hs**

Fechas Inicio Calendario
MCSA y MCSA Security

INICIO	DIAS	HORARIO
03-08-04	M-J	9.00 a 13.00
13-08-04	L-M-V	18.30 a 22.30
12-08-04	M-J	18.30 a 22.30
03-09-04	L-M-V	9.00 a 13.00
09-09-04	M-J	9.00 a 13.00
08-09-04	L-M-V	18.30 a 22.30
05-10-04	M-J	18.30 a 22.30
12-10-04	M-J	9.00 a 13.00
13-10-04	L-M-V	18.30 a 22.30
02-11-04	M-J	9.00 a 13.00
10-11-04	L-M-V	18.30 a 22.30
15-11-04	L-M-V	9.00 a 13.00
04-01-05	M-J	18.30 a 22.30
14-01-05	L-M-V	18.30 a 22.30
19-01-05	L-M-V	9.00 a 13.00
08-02-05	M-J	9.00 a 13.00
11-02-05	L-M-V	9.00 a 13.00
18-02-05	L-M-V	18.30 a 22.30
15-03-05	M-J	9.00 a 13.00
18-03-05	L-M-V	18.30 a 22.30
10-03-05	M-J	18.30 a 22.30
19-04-05	M-J	18.30 a 22.30
14-04-05	M-J	9.00 a 13.00
13-04-05	L-M-V	9.00 a 13.00
04-05-05	M-J	18.30 a 22.30
10-05-05	M-J	9.00 a 13.00
18-05-05	L-M-V	18.30 a 22.30
07-06-05	M-J	9.00 a 13.00
15-06-05	L-M-V	18.30 a 22.30
17-06-05	L-M-V	9.00 a 13.00
05-07-05	M-J	18.30 a 22.30
13-07-05	L-M-V	18.30 a 22.30
15-07-05	L-M-V	9.00 a 13.00

Para más información sobre la carrera MCSA Windows 2003 visitá www.cortech.com.ar/ms/mcsa.htm ó www.microsoft.com/learning/mcp/mcsa/default.asp

Certificaciones Internacionales

¿Dónde se pueden rendir los exámenes para certificarme como MCSA y/o MCSE?

Podés hacer los exámenes en cualquier centro CTEC (Certified Training Education Center) de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com)

Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de 125.00 U$S en U.S.A. por examen; y 80.00 U$S en Argentina (tarifas adicionales o descuentos pueden aplicarse en otras regiones).

Todos los Tracks MCSA

¿Cuáles son los Exámenes que debo tomar para recibirme de MCSA?

Existen muchísimas combinaciones de Exámenes para recibirse de MCSA: Microsoft Certified Systems Administrator. Cada una con diferentes especializaciones y electivos para tomar.

MCSA

http://www.cortech.com.ar/gen/mcsawin2003.pdf
http://www.cortech.com.ar/gen/MCSASec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSAMes2000-2003.pdf

Microsoft Certified Systems Engineer (MCSE) Windows 2003

Microsoft CERTIFIED Technical Education Center

Microsoft CERTIFIED Partner for Learning Solutions

EXAMEN - Client	CURSO - Client
Examen 70–270: Installing, Configuring, and Administering Microsoft Windows XP Professional	**Curso 2285:** Installing, Configuring, and Administering Microsoft Windows XP Professional (Duración **16 hs**)
EXAMEN - Networking	**CURSO - Networking**
Examen 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	**Curso 2273:** Managing and Maintaining a Microsoft Windows Server 2003 Environment (Duración **40 hs**)
Examen 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2276:** Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts (Duración **16 hs**)
	Curso 2277: Implementing, Managing, and Maintaining a MS Windows Server 2003 Network Infrastructure: Network Services (Duración **40 hs**)
Examen 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2278:** Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (Duración **40 hs**)
Examen 70-294: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure	**Curso 2279:** Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure (Duración **40 hs**)
EXAMEN - Design	**CURSO - Design**
Examen 70-298: Designing Security for a Microsoft Windows Server 2003 Network	**Curso 2830:** Designing Security for Microsoft Networks (Duración **24 hs**)
EXAMEN - Elective	**CURSO - Elective**
Examen 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**)

Cursos: 8 (ocho) | **MOC's incluidos: 8 (ocho)** | **Duración Total: 240 hs**

Microsoft Certified Systems Engineer (MCSE Sec.) Security on Windows 2003 (Carrera MCSE + Examen 70-299)

Examen 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network	**Curso 2823:** Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración **40 hs**)

Cursos: 9 (nueve) | **MOC's incluidos: 9 (nueve)** | **Duración Total: 280 hs**

Microsoft Certified Systems Engineer // Track Recomendado // Security + 2282 on Win. 2003 (Carrera MCSE Security + Examen 70-297)

Examen 70-297: Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure	**Curso 2282:** Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure (Duración **40 hs**)

Cursos: 10 (diez) | **MOC's incluidos: 10 (diez)** | **Duración Total: 320 hs**



Fechas Inicio Calendario
MCSE, MCSE Security y MCSE Sec + 2282

INICIO	DIAS	HORARIO
10-08-04	M-J	9.00 a 13.00
20-08-04	L-M-V	18.30 a 22.30
19-08-04	M-J	18.30 a 22.30
10-09-04	L-M-V	9.00 a 13.00
16-09-04	M-J	9.00 a 13.00
15-09-04	L-M-V	18.30 a 22.30
12-10-04	M-J	18.30 a 22.30
19-10-04	M-J	9.00 a 13.00
20-10-04	L-M-V	18.30 a 22.30
09-11-04	M-J	9.00 a 13.00
17-11-04	L-M-V	18.30 a 22.30
24-11-04	L-M-V	9.00 a 13.00
11-01-05	M-J	18.30 a 22.30
21-01-05	L-M-V	18.30 a 22.30
26-01-05	L-M-V	9.00 a 13.00
15-02-05	M-J	9.00 a 13.00
18-02-05	L-M-V	9.00 a 13.00
25-02-05	L-M-V	18.30 a 22.30
22-03-05	M-J	9.00 a 13.00
25-03-05	L-M-V	18.30 a 22.30
17-03-05	M-J	18.30 a 22.30
26-04-05	M-J	18.30 a 22.30
21-04-05	M-J	9.00 a 13.00
20-04-05	L-M-V	9.00 a 13.00
10-05-05	M-J	18.30 a 22.30
17-05-05	M-J	9.00 a 13.00
25-05-05	L-M-V	18.30 a 22.30
14-06-05	M-J	9.00 a 13.00
22-06-05	L-M-V	18.30 a 22.30
24-06-05	L-M-V	9.00 a 13.00
12-07-05	M-J	18.30 a 22.30
20-07-05	L-M-V	18.30 a 22.30
22-07-05	L-M-V	9.00 a 13.00

Para más información sobre la carrera MCSE Windows 2003 visitá www.cortech.com.ar/ms/mcse.htm ó www.microsoft.com/learning/mcp/mcse/default.asp

Todos los Tracks MCSE

¿Cuáles son los Exámenes que debo tomar para recibirme de MCSE?

Existen muchísimas combinaciones de Exámenes para recibirse de MCSE: Microsoft Certified Systems Engineer. Cada una con diferentes especializaciones y electivos para tomar.

MCSE
http://www.cortech.com.ar/gen/mcsewin2003.pdf
http://www.cortech.com.ar/gen/MCSESec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSEMes2000-2003.pdf

Logos MCP

¿Cuáles son los logos que podré utilizar cuándo me reciba de MCP, MCSA, MCSE, MCDBA, MCAD ó MCSD?¿Existe alguna diferencia entre los logos con especializaciones en Security, Messaging, etc..?

Al finalizar de haber rendido todos los Exámenes de cada Carrera Microsoft, podrás utilizar el logo correspondiente. Todos las Carreras (como así tambien las especializaciones) poseen un logo diferente.

Podés encontrar todos los logos Microsoft correspondientes en http://www.microsoft.com/learning/mcpexams/faq/logo.asp

Microsoft Certified Application Developer (MCAD) Visual Basic .NET

Microsoft CERTIFIED Technical Education Center — Microsoft CERTIFIED Partner for Learning Solutions

EXAMEN - Módulo I	CURSO - Módulo I
Examen 70-305: Developing and Implementing Web Applications with Microsoft® Visual Basic® .NET and Microsoft® Visual Studio® .NET	**Curso 2559:** Introduction to Visual Basic .NET Programming with Microsoft .NET (Duración **20 hs**) **Curso 2310:** Developing Microsoft ASP.NET Web Applications Using Visual Studio .NET (Duración **40 hs**)
EXAMEN - Módulo II	**CURSO - Módulo II**
Examen 70-310: Developing XML Web Services and Server Components with Microsoft® Visual Basic® .NET and the Microsoft® .NET Framework	**Curso 2415:** Programming with the Microsoft® .NET Framework (Microsoft V. Basic® .NET) (Duración **40 hs**) **Curso 2524:** Developing XML Web Services Using Microsoft® ASP.NET (Duración **20 hs**) **Curso 2557:** Building COM+ Applications Using Microsoft® .NET Enterprise Services (Duración **20 hs**)
EXAMEN - Módulo III	**CURSO - Módulo III**
Examen 70-229: Designing and Impl. Databases with MS SQL Server 2000™ Enterprise Edition	**Curso 2073:** Programming a Microsoft SQL Server 2000 Database (Duración **40 hs**)
# Cursos: 6 (seis) **MOC's incluidos: 6 (seis)**	**Duración Total: 180 hs**

SQL Server

Las dos Certificaciones de SQL más importantes son: **Examen 70-228** (Installing, Configuring, and Administering Microsoft SQL Server 2000 Enterprise Edition) y **Examen 70-229** (Designing and Implementing Databases with Microsoft SQL Server 2000 Enterprise Edition).

Estos Exámenes podrán prepararse con los Cursos Oficiales **2072** (Administering a MS-SQL Server 2000 Database) y **2073** (Programming a MS-SQL Server 2000 Database) respectivamente.

Microsoft Certified Solution Developer (MCSD) Visual Basic .NET (Carrera MCAD + Examen 70-300 + Examen 70-306)

EXAMEN - Módulo IV	CURSO - Módulo IV
Examen 70-300: Analyzing Requirements & Defining .NET Solution Architectures	**Curso 2710 :** Analyzing Requirements and Defining .NET Solution Architecture (Duración **40 hs**)
EXAMEN - Módulo V	**CURSO - Módulo V**
Examen 70-306: Developing & Impementing Windows-based Applications with Microsoft Visual Basic .NET & MS Visual Studio .NET	**Curso 2565:** Developing Microsoft .NET Applications for Windows (Visual Basic .NET) (Duración **20 hs**)
# Cursos: 8 (ocho) **MOC's incluidos: 8 (ocho)**	**Duración Total: 240 hs**

Fechas Inicio Calendario
MCAD V. Basic, MCSD y MCAD C#

INICIO	DIAS	HORARIO
03-08-04	M-J	9.00 a 13.00
13-08-04	L-M-V	18.30 a 22.30
12-08-04	M-J	18.30 a 22.30
03-09-04	L-M-V	9.00 a 13.00
09-09-04	M-J	9.00 a 13.00
08-09-04	L-M-V	18.30 a 22.30
05-10-04	M-J	18.30 a 22.30
12-10-04	M-J	9.00 a 13.00
13-10-04	L-M-V	18.30 a 22.30
02-11-04	M-J	9.00 a 13.00
10-11-04	L-M-V	18.30 a 22.30
15-11-04	L-M-V	9.00 a 13.00
04-01-05	M-J	18.30 a 22.30
14-01-05	L-M-V	18.30 a 22.30
19-01-05	L-M-V	9.00 a 13.00
08-02-05	M-J	9.00 a 13.00
11-02-05	L-M-V	9.00 a 13.00
18-02-05	L-M-V	18.30 a 22.30
15-03-05	M-J	9.00 a 13.00
18-03-05	L-M-V	18.30 a 22.30
10-03-05	M-J	18.30 a 22.30
19-04-05	M-J	18.30 a 22.30
14-04-05	M-J	9.00 a 13.00
13-04-05	L-M-V	9.00 a 13.00
04-05-05	M-J	18.30 a 22.30
10-05-05	M-J	9.00 a 13.00
18-05-05	L-M-V	18.30 a 22.30
07-06-05	M-J	9.00 a 13.00
15-06-05	L-M-V	18.30 a 22.30
17-06-05	L-M-V	9.00 a 13.00
05-07-05	M-J	18.30 a 22.30
13-07-05	L-M-V	18.30 a 22.30
15-07-05	L-M-V	9.00 a 13.00

Microsoft Certified Application Developer (MCAD) C#™ .NET

// Track Recomendado //

EXAMEN - Módulo I	CURSO - Módulo I
Examen 70-315: Developing and Implementing Web Applications with Microsoft Visual C#™ .NET and Microsoft Visual Studio .NET	**Curso 2609:** Introduction to C# Programming with Microsoft .NET (Duración **20 hs**) **Curso 2310:** Developing Microsoft ASP.NET Web Applications Using Visual Studio .NET (Duración **40 hs**)
EXAMEN - Módulo II	**CURSO - Módulo II**
Examen 70-320: Developing XML Web Services and Server Components with Microsoft Visual C# and the Microsoft .NET Framework	**Curso 2349:** Programming with the Microsoft .NET Framework (Microsoft Visual C# .NET).(Duración **40 hs**) **Curso 2524:** Developing XML Web Services Using Microsoft® ASP.NET (Duración **20 hs**) **Curso 2557:** Building COM+ Applications Using Microsoft® .NET Enterprise Services (Duración **20 hs**)
EXAMEN - Módulo III	**CURSO - Módulo III**
Examen 70-229: Designing and Impl. Databases with MS SQL Server 2000™ Enterprise Edition	**Curso 2073:** Programming a Microsoft SQL Server 2000 Database (Duración **40 hs**)
# Cursos: 6 (seis) **MOC's incluidos: 6 (seis)**	**Duración Total: 180 hs**

Para más información sobre la carrera MCAD .NET, MCSD y MCAD C# visitá www.cortech.com.ar/ms/ms4.htm ó www.microsoft.com/learning/mcp/mcad/

Links Microsoft

¿Existe algún link en donde se puedan ver todos los Exámenes actuales de Microsoft y todos sus Cursos Oficiales asociados?

Para ver todos los Exámenes Microsoft vigentes que existen visitá **www.microsoft.com/learning/mcpexams/prepare/findexam.asp** Allí los podrás visualizar por Carreras o por número de Examen.

Y para ver todos los Cursos Oficiales vigentes visitá **www.microsoft.com/traincert/training/find/findcourse.asp** Allí podrás visualizarlos por Producto o por número de Curso.

Carrera MCDBA

¿Cuáles son los exámenes que debo tomar para realizar la Carrera MCDBA?

Para ver el listado completo de todas las opciones que existen para convertirte en Microsoft Certified Data Base Administrator (MCDBA) te recomendamos visitar la siguiente página WEB: http://www.microsoft.com/learning/mcp/mcdba/default.asp.

El Track recomendado para convertirte en MCDBA es realizar la Carrera MCSE de 240 hs de Duración (7 Exámenes) + los Exámenes de SQL Server 70-228 (Administering) y 70-229 (Programming)

Fechas Inicio Calendario
WEB Design Completa y Expert

INICIO	DIAS	HORARIO
06-08-04	L-M-V	9.30 a 12.30
12-08-04	M-J	18.30 a 21.30
17-08-04	M-J	14.00 a 17.00
04-09-04	S	10.00 a 13.00
08-09-04	L-M-V	18.30 a 21.30
16-09-04	M-J	9.30 a 12.30
01-10-04	L-M-V	9.30 a 12.30
07-10-04	M-J	18.30 a 21.30
13-10-04	L-M-V	14.00 a 17.00
06-11-04	S	10.00 a 13.00
10-11-04	L-M-V	18.30 a 21.30
18-11-04	M-J	9.30 a 12.30
07-01-05	L-M-V	9.30 a 12.30
13-01-05	M-J	18.30 a 21.30
18-01-05	M-J	14.00 a 17.00
05-02-05	S	10.00 a 13.00
11-02-05	L-M-V	18.30 a 21.30
17-02-05	M-J	9.30 a 12.30
04-03-05	L-M-V	9.30 a 12.30
17-03-05	M-J	18.30 a 21.30
18-03-05	L-M-V	14.00 a 17.00
09-04-04	S	10.00 a 13.00
08-04-05	L-M-V	18.30 a 21.30
21-04-05	M-J	9.30 a 12.30
13-05-04	L-M-V	9.30 a 12.30
12-05-05	M-J	18.30 a 21.30
19-05-05	M-J	14.00 a 17.00
11-06-05	S	10.00 a 13.00
15-06-05	L-M-V	18.30 a 21.30
16-06-05	M-J	9.30 a 12.30
06-07-05	L-M-V	9.30 a 12.30
14-07-05	M-J	18.30 a 21.30
20-07-05	L-M-V	14.00 a 17.00

Carrera WEB Design Completa
WEB1 + WEB2 + WEB3

EXAMEN - WEB Design	CURSO - WEB Design
Examen Dreamweaver MX 2004 Designer	**Módulo WEB1:** Curso de Front Page XP y Macromedia Dreamweaver MX 04 (Duración **18 hs**)
Exámenes Flash MX 2004 Designer y Developer	**Módulo WEB2:** Curso de Macromedia Flash MX 04 y Macromedia Fireworks MX 04 (Duración **21 hs**)
Exámenes Dreamweaver MX 2004 Designer y Developer	**Módulo WEB3:** Curso de Edición HTML e Introd. a Programación ASP (Duración **21 hs**)

Cursos: 3 (tres) **WOG's incluidos: 1 (uno)** **Duración Total: 60 hs**

Carrera WEB Design Expert
WEB1 + WEB2 + WEB3 + WEB4 + WEB5 // Track Recomendado //

EXAMEN - WEB Design	CURSO - WEB Developer
Examen Dreamweaver MX 2004 Developer	**Módulo WEB4:** Curso Programación ASP Avanzado (Duración **21 hs**)
-- --	**Módulo WEB5:** Curso Programación PHP Avanzado (Duración **21 hs**)

Cursos: 5 (cinco) **WOG's incluidos: 2 (dos)** **Duración Total: 102 hs**

Para más información sobre la carrera WEB Design Completa y WEB Design Expert visitá www.cortech.com.ar/web/web1.htm



Fechas Inicio Calendario
Carrera COR Security + Especializaciones

INICIO	DIAS	HORARIO
17-08-04	M-J	9.00 a 13.00
27-08-04	L-M-V	18.30 a 22.30
26-08-04	M-J	18.30 a 22.30
17-09-04	L-M-V	9.00 a 13.00
23-09-04	M-J	9.00 a 13.00
22-09-04	L-M-V	18.30 a 22.30
19-10-04	M-J	18.30 a 22.30
26-10-04	M-J	9.00 a 13.00
27-10-04	L-M-V	18.30 a 22.30
16-11-04	M-J	9.00 a 13.00
24-11-04	L-M-V	18.30 a 22.30
29-11-04	L-M-V	9.00 a 13.00
18-01-05	M-J	18.30 a 22.30
28-01-05	L-M-V	18.30 a 22.30
02-02-05	L-M-V	9.00 a 13.00
22-02-05	M-J	9.00 a 13.00
25-02-05	L-M-V	9.00 a 13.00
04-03-05	L-M-V	18.30 a 22.30
29-03-05	M-J	9.00 a 13.00
23-03-05	L-M-V	18.30 a 22.30
24-03-05	M-J	18.30 a 22.30
14-04-05	M-J	18.30 a 22.30
28-04-05	M-J	9.00 a 13.00
27-04-05	L-M-V	9.00 a 13.00
17-05-05	M-J	18.30 a 22.30
24-05-05	M-J	9.00 a 13.00
01-06-05	L-M-V	18.30 a 22.30
21-06-05	M-J	9.00 a 13.00
29-06-05	L-M-V	18.30 a 22.30
01-07-05	L-M-V	9.00 a 13.00
19-07-05	M-J	18.30 a 22.30
27-07-05	L-M-V	18.30 a 22.30
29-07-05	L-M-V	9.00 a 13.00

Carrera COR Security // Track Recomendado //
SEC1 + SEC2 + Especialización (a elección)

EXAMEN - CISSP	CURSO - Security
 CISSP: Certified Information Systems Security Professional	**Clínica SEC1:** Seguridad y sus fundamentos (Duración **20 hs**) **Clínica SEC2:** Seguridad Avanzada (Duración **20 hs**)
Especialización LINUX	**Especialización Microsoft**
Módulo LX5: Seguridad y contra-seguridad en Redes (Duración **12hs**) + **Workshop LX6:** Workshops Servidor de Firewall y Squid (Comparación con ISA Server) (Duración **12 hs**) + **Workshop LX8:** Workshops Implementando VPNs bajo Linux (Duración **12 hs**)	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**) + **Curso 40 hs Seguridad Electivo** de la Currícula Oficial Microsoft + **Curso 2823:** Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración **40 hs**)
Incluye Material **# Cursos: 5 (cinco)** **Duración Total: 76 hs**	**Incluye Material** **# Cursos: 5 (cinco)** **Duración Total: 144 hs**

Para más información sobre la carrera COR Security y sus Especializaciones visitá www.secure105.com.ar

Cursos Intensivos y Personalizados

¿Cómo puedo hacer para que yo o la gente de mi Empresa pueda cursar cualquiera de los Cursos y Carreras Microsoft, Security, WEB Design o Linux de manera Personalizada / Intensiva?

Te recomendamos averiguar por costos y metodologías de cursada de todos nuestros Cursos y Carreras para realizarlos de forma intensiva y personalizada ya sea en las Oficinas de COR TECH o in Company (Capital o Interior del País).
Enviando solamente un email a intensive@cortech.com.ar o llamando al (54)11-4312-7694.

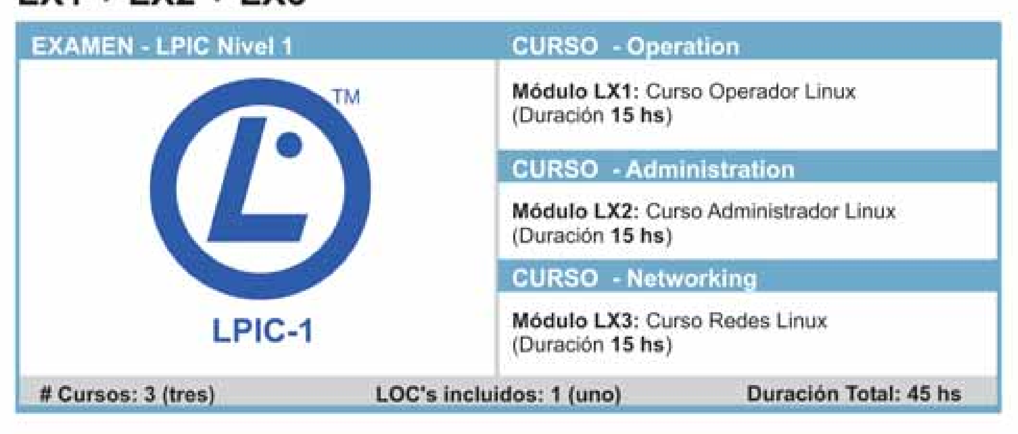
Certificaciones Macromedia

¿Dónde se pueden rendir los exámenes para certificarme como Macromedia Dreamweaver MX 2004 Designer, Developer y Flash MX 2004 Designer, Developer?

Podés hacer los exámenes en cualquier centro de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com). Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de 150.00 U$S para cada Examen MX 2004.

Más información respecto de las Certificaciones Macromedia MX 2004 podrás encontrarla en **www.macromedia.com**

Carrera Linux Completa
LX1 + LX2 + LX3



EXAMEN - LPIC Nivel 1	CURSO - Operation
LPIC-1	**Módulo LX1:** Curso Operador Linux (Duración **15 hs**)
	CURSO - Administration
	Módulo LX2: Curso Administrador Linux (Duración **15 hs**)
	CURSO - Networking
	Módulo LX3: Curso Redes Linux (Duración **15 hs**)

Cursos: 3 (tres) **LOC's incluidos: 1 (uno)** **Duración Total: 45 hs**

Carrera Linux Avanzada
LX1 + LX2 + LX3 + LX4 + LX5



EXAMEN - LPIC Nivel 2	CURSO - Networking
LPIC-2	**Módulo LX4:** Curso Redes Linux Avanzado (Duración **15 hs**)
	CURSO - Securing
	Módulo LX5: Curso Seguridad y Contra-Seguridad Linux (Duración **15 hs**)

Cursos: 5 (cinco) **LOC's incluidos: 2 (dos)** **Duración Total: 69 hs**

Carrera Linux Expert // Track Recomendado //
LX1 + LX2 + LX3 + LX4 + LX5 + 2 Workshops LX (a elección)



EXAMEN - LPIC Nivel 1 y Nivel 2	Workshops - Certificación
LPIC-1 LPIC-2	**LPIC-1:** Workshops para Exámenes LPI-101 y LPI-102 (Duración **12 hs**)
	LPIC-2: Workshops para Exámenes LPI-201 y LPI-202 (Duración **12 hs**)
EXAMEN - LPIC Nivel 3	**Workshops - Expert Linux**
LPIC-3	**LX6:** Workshops Servidor de Firewall y Squid (Comparación con ISA Server) (Duración **12 hs**)
	LX7: Workshops Clustering bajo Linux (Beowulf/ Open Mosix / Condor) (Duración **12 hs**)
	LX8: Workshops Implementando VPNs bajo Linux (FreeSwan) (Duración **12 hs**)
	LX9: Workshops Apache WEB Server (Duración **12 hs**)

Cursos: 7 (siete) **LOC's incluidos: 4 (cuatro)** **Duración Total: 93 hs**

debian





Fechas Inicio Calendario
Carrera Linux Complete, Advanced y Expert

INICIO	DIAS	HORARIO
11-08-04	L-M-V	9.30 a 12.30
14-08-04	S	10.00 a 13.00
17-08-04	M-J	18.30 a 21.30
03-09-04	L-M-V	18.30 a 21.30
09-09-04	M-J	9.30 a 12.30
14-09-04	M-J	14.00 a 17.00
06-10-04	L-M-V	9.30 a 12.30
09-10-04	S	10.00 a 13.00
14-10-04	M-J	18.30 a 21.30
05-11-04	L-M-V	18.30 a 21.30
11-11-04	M-J	9.30 a 12.30
12-11-04	L-M-V	14.00 a 17.00
05-01-05	L-M-V	9.30 a 12.30
08-01-05	S	10.00 a 13.00
13-01-05	M-J	18.30 a 21.30
04-02-05	L-M-V	18.30 a 21.30
10-02-05	M-J	9.30 a 12.30
15-02-05	M-J	14.00 a 17.00
04-03-05	L-M-V	9.30 a 12.30
12-03-05	S	10.00 a 13.00
17-03-05	M-J	18.30 a 21.30
06-04-05	L-M-V	18.30 a 21.30
14-04-05	M-J	9.30 a 12.30
08-04-05	L-M-V	14.00 a 17.00
04-05-05	L-M-V	9.30 a 12.30
07-05-05	S	10.00 a 13.00
12-05-05	M-J	18.30 a 21.30
08-06-05	L-M-V	9.30 a 12.30
09-06-05	M-J	18.30 a 21.30
14-06-05	M-J	14.00 a 17.00
01-07-05	L-M-V	18.30 a 21.30
14-07-05	M-J	9.30 a 12.30
16-07-05	S	10.00 a 13.00

Para más información sobre la carrera Linux Completa, Avanzada y Expert visitá www.cortech.com.ar/lxc/lxc1.htm

Costos de las Carreras y Cursos

¿Dónde se puede averiguar el costo de los Cursos y Carreras Microsoft, Security, WEB Design y/o Linux?

Podés averiguar los costos de los Cursos y Carreras acercándote personalmente a COR Technologies SRL: Av. Córdoba 657 Piso 12, telefónicamente llamando al (54)11-4312-7694, vía correo electrónico a masinfo@cortech.com.ar, o en http://www.cortech.com.ar

http://www.cortech.com.ar/gen/Cursos y Fechas COR.pdf

Certificaciones LPI

¿Dónde se pueden rendir los exámenes para certificarme en LPIC 101, 102, 201 ó 202?

Podés hacer los exámenes en cualquier centro de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com)

Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de 150.00 U$S para cada Examen.

Más información respecto de las Certificaciones LPI podrás encontrarla en **www.lpi.org**









Revista de Networking y Programación
www.nexweb.com.ar

NEX # 11 - Septiembre 2004- Precio Argentina 4 $ (recargo interior del País 0,20 $) / Bolivia 10 $ / Chile 1500 $ / México 15 $ / Paraguay 9000 Gs / Uruguay 35 $ / Perú 5.5 ns / Venezuela 2000 bs.

FreeBSD, OpenBSD y netBSD

Cracking Passwords

LC5 y Rainbowcrack

Ethical Hacking: Scanning con nmap

VPNs en LINUX

Super-Free SWAN y Open SWAN

Clusters bajo Windows



ISSN 1668-5423







